

Ira M. Siegel, Cal. State Bar No. 78142
email address: irasiegel@earthlink.net
LAW OFFICES OF IRA M. SIEGEL
433 N. Camden Drive, Suite 970
Beverly Hills, California 90210-4426
Tel: 310-435-7656
Fax: 310-657-2187

Attorney for Plaintiff Digital Sin, Inc.

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

Digital Sin, Inc.,
a California corporation,

Plaintiff,

v.

DOES 1-5698,

Defendants.

CASE NO. CV 11-4397 LB

**PLAINTIFF'S EX PARTE
APPLICATION FOR LEAVE TO
TAKE LIMITED DISCOVERY PRIOR
TO A RULE 26(f) CONFERENCE**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND FACTS–PLAINTIFF NEEDS THE ASSISTANCE OF COURTS TO ENFORCE ITS COPYRIGHTS AGAINST MASS COPYRIGHT INFRINGEMENT	1
III.	ARGUMENT	7
A.	A Court May Allow Early Discovery, and Should Do So in this Case	7
B.	The Discovery Sought by Plaintiff Is Reasonably Likely to Lead to Identifying Information About Defendant That Would Make Service of Process Possible.....	9
C.	Neither First Amendment Nor Privacy Rights Preclude Discovery	10
	1. First Amendment Rights Are Not Abrogated Here	10
	2. Privacy Rights Are Not Abrogated Here	10
	(a) There Is No Reasonable Expectation of Privacy Here.....	10
	(b) 47 U.S.C. § 551 Does Not Preclude Compliance With the Subpoenas	10
	3. Joinder of Defendants Is Appropriate, and, Even If in Doubt, Should Not Be a Bar to the Discovery Sought at This Stage of Litigation	11
	4. Consideration of the Personal Jurisdiction Issue at this Stage of Litigation Is Premature	19
D.	The Exemplary Subpoena Will Elicit the Required Information	23
IV.	THERE IS NO NEED FOR TENDERING WITNESS AND MILEAGE FEES	24
V.	CONCLUSION.....	25

TABLE OF CASES

1		
2	<u>Apple Computer, Inc. v. Franklin Computer Corp.</u> , 714 F.2d 1240	
3	(3d Cir. 1983).....	8
4	<u>BMG Music v. Does</u> , No. C 06-01579, 2006 U.S. Dist. LEXIS 53237	
5	(N.D. Cal. Jul. 31, 2006).....	14
6	<u>Calder v. Jones</u> , 465 U.S. 783, 79 L. Ed. 2d 804, 104 S. Ct. 1482 (1984)	23
7	<u>Call of the Wild Movie, LLC v. Does 1-1,062</u> , 770 F. Supp. 2d 332	
8	(D.D.C. March 22, 2011)	5,13-14,20-22
9	<u>Columbia Ins. Co. v. Seescandy.com</u> , 185 F.R.D. 573 (N.D. Cal.	
10	1999)	8,9
11	<u>Gillespie v. Civiletti</u> , 629 F.2d 637 (9th Cir. 1980)	8,9
12	<u>Hard Drive Productions v. Does 1-42</u> , N.D. Cal. Case No. CV 11-	
13	01956 EDL (N.D. Cal. Decided August 3, 2011) Doc. #20	18
14	<u>Interscope Records v. Does 1-25</u> , No. 6:04-cv-197, 2004 U.S. Dist.	
15	LEXIS 27782 (M.D. Fla. Apr. 1, 2004).....	14
16	<u>IO Group, Inc. v. Pivotal</u> , No. C 03-5286 MHP, 2004 U.S. Dist.	
17	LEXIS 6673, 2004 WL 838164, *6 (N.D. Cal. Apr. 19, 2004).....	23
18	<u>LaFace Records, LLC v. Does 1-38</u> , No. 5:07-cv-298, 2008 WL	
19	544992, 2008 U.S. Dist. LEXIS 14544 (E.D. N.C. Feb. 27, 2008).....	14
20	<u>Martindale v. Windsor</u> , 75 F.R.D. 665 (D. Colo. 1997)	25
21	<u>MCGIP, LLC v. Does 1-18</u> , 2011 U.S. Dist. LEXIS 64188 (N.D. Cal.	
22	June 2, 2011)	5,16,19
23	Northern District of California Case No. CV 10-05863 MEJ	14
24	Northern District of California Case No. CV 10-05865-PSG	14
25	Northern District of California Case No. CV 10-05885 JCS.....	14
26	<u>Semitool, Inc. v. Tokyo Electron Am., Inc.</u> , 208 F.R.D. 273 (N.D.	
27	Cal. 2002).....	8
28	<u>Sony Music Entertainment Inc. v. Does 1-40</u> , 326 F. Supp. 2d 556	
	(S.D.N.Y. 2004)	10,20
	<u>Twentieth Century Fox Film Corp. v. Does 1-12</u> , No. C 04-04862	
	WHA (N.D. Cal. Nov. 16, 2004)	14
	<u>UMG Recordings, Inc. v. Does 1-4</u> , No. 06-0652 SBA, 2006 U.S.	
	Dist. LEXIS 32821 (N.D. Cal. Mar. 6, 2006)	10
	<u>United Mine Workers of Am. v. Gibbs</u> , 383 U.S. 715 (1966).....	12
	<u>Voltage Pictures, LLC v. Does 1-5000</u> , 2011 U.S. Dist. LEXIS	
	50787 (D.D.C. May 12, 2011)	16,17,22
	<u>Yokohama Tire Corp. v. Dealers Tire Supply, Inc.</u> , 202 F.R.D. 612	
	(D. Ariz. 2001)	8

TABLE OF STATUTES AND RULES

Article I, Section 8, Clause 8 of the United States Constitution.....	4
First Amendment of the United States Constitution.....	10
17 U.S.C. § 101 et seq.....	4
17 U.S.C. § 106.....	9
47 U.S.C. § 551 (Cable Communications Policy Act of 1984).....	10,11
Rule 6(c)(1)(C) of the Federal Rules of Civil Procedure.....	1
Rule 20 of the Federal Rules of Civil Procedure.....	11,12
Rule 26 of the Federal Rules of Civil Procedure.....	1,7,23
Rule 45 of the Federal Rules of Civil Procedure.....	7,19,20,23,24,25

I. INTRODUCTION

Plaintiff Digital Sin, Inc. is a motion picture production company. The work at issue in this case (the "Work") is titled "My Little Panties #2" and is registered in the United States Copyright Office: Registration Number PA 1-733-587. The Work and the copyright therein are owned by Plaintiff. Complaint, par. 7 and 8. Declaration of Jon Nicolini, par. 10 and 13.

Plaintiff makes this Ex Parte Application for Leave to Take Limited Discovery Prior to a Rule 26 Conference because, without such discovery, Plaintiff will not be able to identify the Defendants with sufficient particularity to effect service of process. This Ex Parte Application is supported by the memorandum set forth below and the concurrently-filed Nicolini Declaration.

Plaintiff could not obtain a stipulation for this Ex Parte Application because Plaintiff cannot identify the Doe defendants with whom to confer until the requested discovery occurs.

Federal Rule 6(c)(1)(C) of the Federal Rules of Civil Procedure, relating to times for filing motions and setting hearings, provides that for good cause a party may apply ex parte for setting a different time to file a motion with respect to a hearing date. Because there is currently no Defendant in this case to oppose any motion, or upon whom to serve a copy of a motion or ex parte application, there would be no opposition if a motion were filed instead of an ex parte application. Therefore, no briefing schedule need be set.

II. BACKGROUND FACTS—PLAINTIFF NEEDS THE ASSISTANCE OF COURTS TO ENFORCE ITS COPYRIGHTS AGAINST MASS COPYRIGHT INFRINGEMENT

This copyright infringement case involves motion picture mass piracy of the kind that has been plaguing the country as advances in technology have made infringements almost effortless to accomplish at the same time that identifying the infringers has become more difficult. This mass piracy is conducted by numerous people participating in a "swarm" of infringers who use the Internet to illegally copy and distribute motion pictures.¹

¹ "Swarm" thievery enabled by the Internet is not limited to copyright infringement. "Swarm" or "flash mob" shoplifting cases occur. See the reports at the following web pages about swarm shoplifting events in Washington, D.C., Las Vegas, NV, and St. Paul, MN:

http://www.myfoxdc.com/dpp/news/dc/video-mob-of-teens-rob-dupont-circle-store-042711?utm_medium=twitter&utm_source=twitterfeed

http://www.cbsnews.com/8301-504083_162-20060576-504083.html

<http://www.myfoxtwincities.com/dpp/news/minnesota/st.-paul-stores-suffer-'mob-thefts'-feb-22-2011>

1 The Variety article is attached hereto as Exhibit 6 and can be seen here,

2 <http://www.variety.com/article/VR1118035369>.

3 Note that Vice President Biden was talking about everyday people committing piracy.
 4 One of the biggest, if not the biggest, means by which copyright "pirates" engage in theft of
 5 motion pictures is through peer-to-peer networks on the Internet. See, the January 2011 Report
 6 by Envisional Ltd. that was commissioned by NBC Universal to analyze bandwidth usage across
 7 the Internet with the specific aim of assessing how much of that usage infringed upon copyright.

8 The Envisional Report can be seen here,

9 http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf

10 and is attached hereto as Exhibit 8.

11 Key findings set out in the Envisional Report include these:

- 12 • Across all areas of the global internet, 23.76% of traffic was estimated to be
- 13 infringing. This excludes all pornography, the infringing status of which can
- 14 be difficult to discern.
- 15 • The level of infringing traffic varied between internet venues and was highest
- 16 in those areas of the internet commonly used for the distribution of pirated
- 17 material.
- 18 • BitTorrent traffic is estimated to account for 17.9% of all internet traffic.
- 19 Nearly two-thirds of this traffic is estimated to be non-pornographic
- 20 copyrighted content shared illegitimately such as films, television episodes,
- 21 music, and computer games and software (63.7% of all bittorrent traffic or
- 22 11.4% of all internet traffic).
- 23 * * *
- 24 • In the United States, 17.53% of Internet traffic was estimated to be infringing.
- 25 This excludes all pornography. A breakdown of internet usage yields the
- 26 following results:
- 27 • Peer to peer networks were 20.0% of all internet traffic with bittorrent
- 28 responsible for 14.3%. The transfer of infringing content located on these
- networks comprised 13.8% of all internet traffic.
- As would be expected of copyright pirates, they do not come forward and
- openly identify themselves, and many behave with the implicit understanding
- that catching them would be difficult.
- 29 * * *
- 30 BitTorrent
- 31 • BitTorrent is the most used file sharing protocol worldwide with over 8m
- 32 simultaneous users and 100m regular users worldwide.
- 33 • Over 2.72m torrents managed by the largest bittorrent tracker were examined
- 34 for this report. Our analysis suggests nearly two-thirds of all content shared on
- 35 bittorrent is copyrighted and shared illegitimately.
- 36 • An in-depth analysis of the most popular 10,000 pieces of content managed by
- 37 PublicBT found:
- 38 • 63.7% of content managed by PublicBT was non-pornographic content
- that was copyrighted and shared illegitimately

- 35.2% was film content – all of which was copyrighted and shared illegitimately
- 14.5% was television content – all of which was copyrighted and shared illegitimately. Of this, 1.5% of content was Japanese anime and 0.3% was sports content.
- 6.7% was PC or console games - all of which was copyrighted and shared illegitimately
- 2.9% was music content – all of which was copyrighted and shared illegitimately
- 4.2% was software – all of which was copyrighted and shared illegitimately
- 0.2% was book (text or audio) or comic content – all of which was copyrighted and shared illegitimately
- 35.8% was pornography, the largest single category. The copyright status of this was more difficult to discern but the majority is believed to be copyrighted and most likely shared illegitimately⁴
- 0.48% (just 48 files out of 10,000) could not be identified

⁴For the purposes of this report, the copyright status of any pornography identified is ignored, though the piracy of such content is obviously of interest to the adult video industry (reflected in the many legal suits filed against downloaders during 2010).

Envisional Report, pp. 2-5. (Emphasis omitted, some footnotes omitted.)

The Constitution at Article I, Section 8, Clause 8, empowers Congress to provide for an author's exclusive rights to his works. The tool Congress provided to fight all this piracy is the Copyright Act, 17 U.S.C. §§ 101 etc., and copyright owners must themselves, pursuant to the Act, engage the United States District Courts to enforce their rights.

As is clear from the statements of Vice President Biden and former Senator Dodd, movie studios such as Plaintiff are suffering greatly from the fact that a great many people are willing to thumb their noses at the Constitution and the Congressionally enacted Copyright Act now that they have a way of semi-anonymously pirating works through the Internet. **Copyright owners such as Plaintiff obviously need the assistance of courts, and not judicial obstacles put in the way of copyright enforcement.**

In Call of the Wild Movie, LLC v. Does 1-1,062, 770 F. Supp. 2d 332 (D.D.C. March 22, 2011)², in an opinion relating to three cases with a total of 5583 Doe defendants involved, U.S. District Judge Beryl Howell noted as follows at p. 345:

² Call of the Wild Movie, was favorably cited by United States District Judge Edward M. Chen in MCGIP, LLC v. Does 1-18, 2011 U.S. Dist. LEXIS 64188 [*2] (N.D. Cal. June 2, 2011). While Judge Chen noted that the case before him did not include 100s or 1000s of Doe defendants, the reasoning used by him would be the same even if that many Doe defendants were included.

1 "Given the administrative burden of simply obtaining sufficient
2 identifying information to properly name and serve alleged infringers, it is highly
3 unlikely that the plaintiffs could protect their copyrights in a cost-effective
4 manner. Indeed, Time Warner urges the Court to sever the defendants for this
very reason. Time Warner asserts that, if joinder were disallowed, its burden of
complying with subpoenas would be diminished because the plaintiffs would not
be able to proceed against all of the putative defendants individually."

5 In that case, ISP Time Warner Cable sought to quash the subpoenas seeking information about
6 the Doe defendants' identities. Three putative defendants whose identities were disclosed, and
7 amici Electronic Frontier Foundation, Public Citizen, ACLU Foundation, and American Civil
8 Liberties Union of the Nation's Capital, unsuccessfully supported Time Warner Cable's motion to
9 quash, challenging, among other things, personal jurisdiction over doe defendants that likely
10 resided outside of the district in which the litigation was pending.

11 In the instant case, Defendants Does 1-5698, many of whom are likely residents of this
12 judicial district, have, without the consent of Plaintiff, cooperatively acted with each other to
13 distribute among themselves unauthorized copies of the Work. On information and belief, more
14 than 1 out of every 4 of the Defendants' IP addresses is physically located in California, and of
15 those, more than 1 out of every 4 is in this judicial district. Complaint, par. 10 and 11. Nicolini
16 Decl., par. 23.

17 Defendants engaged and continue to engage in infringement of Plaintiff's copyright
18 through online media distribution systems. Users such as Defendants download software to their
19 computers that allows them to join file-sharing networks, often referred to as a "peer to peer" or a
20 "P2P" networks, to locate and transfer files to and from other users. In order to use the software
21 to locate and exchange files, a user connects to the Internet. Nicolini Decl., par. 4-9.

22 Users subscribe to the services of an Internet Service Provider ("ISP"), such as the ISPs
23 listed in **Exhibit A** attached to the Complaint (and, for the Court's convenience, to the Nicolini
24 Declaration), to gain access to the Internet. Each time a subscriber accesses the Internet, the ISP
25 provides a unique Internet Protocol ("IP") address to the subscriber. An ISP generally records
26 the times and dates that it assigns each IP address to a subscriber and maintains for a period of
27 time a record of such an assignment in logs maintained by the ISP. In addition, the ISP
28

1 maintains records which typically include the name, one or more address, one or more telephone
2 numbers, and one or more email addresses of the subscriber. Nicolini Decl., par. 18.

3 P2P technology relies on the ability to identify the computers to and from which users
4 can search and exchange files. The technology identifies those computers by the IP address from
5 which the computer connects to the Internet. Taking advantage of this technology, Plaintiff's
6 contractor, Copyright Enforcement Group, LLC ("CEG"), inspects file-sharing networks for
7 computers that are distributing at least a substantial portion of a copy of a copyrighted work
8 owned by Plaintiff, and when CEG finds such a computer, CEG records the IP address of the
9 computer and the date and time ("Timestamp") of the recording. In addition, CEG uses available
10 databases to record the name of the ISP having control of the IP address and the state (and often
11 the city) associated with that IP address. However, because of the partially anonymous nature of
12 the P2P Internet distribution system used by Defendants, the true names, street addresses,
13 telephone numbers and email addresses of Defendants are unknown to Plaintiff at this time.
14 CEG also downloads the available file from a subscriber's computer, and later runs visual
15 observations to confirm whether or not the file is a copy of at least a substantial portion of a
16 copyrighted work of Plaintiff. CEG has confirmed that each of the files obtained from the
17 Defendants that are listed in **Exhibit A** to the Complaint is a copy of a substantial portion of the
18 copyrighted work listed in **Exhibit A**. Nicolini Decl., par. 17-19, and 22.

19 ISPs maintain for certain periods of time subscriber activity logs that contain information
20 linking an IP address and the Timestamp to the identity of the Defendant-subscriber. At some
21 point in time, ISPs typically destroy such information. ISPs also maintain records that include
22 their respective subscribers names, addresses, telephone numbers, and email addresses. With an
23 IP address and Timestamp, the ISP having control of an IP address can identify and produce the
24 logs and records that include the Defendant's name, address, telephone number, and email
25 address. Currently, that information (i.e., subscriber identifying information associated with
26 each IP address/Timestamp combination) is known by, and only by, the ISP. Nicolini Decl., par.
27 18-20, and 22.

Exhibit A lists on a Defendant-by-Defendant basis (one Defendant per row) the IP address associated with each Defendant, the identity of the ISP associated with the IP address, the date and time (the Timestamp referred to earlier) that the infringement by that Defendant was last observed, and the software protocol used by the Defendant in infringing the Work, the title of which, along with its copyright registration number, is set forth on the first page of **Exhibit A**. Nicolini Decl., par. 21.

Plaintiff seeks leave from the Court to serve a Rule 45 third-party subpoena on each ISP listed in **Exhibit A** prior to a Rule 26 Case Management Conference.

III. ARGUMENT

A. A Court May Allow Early Discovery, and Should Do So in this Case

Rule 26(d) of the Federal Rules of Civil Procedure provides that, unless authorized by, among other authorities, a court order, discovery from no source may be had until the parties have conferred as required by Rule 26(f).

Here, of course, because of the semi-anonymity of the Defendants, no meeting with any of them can be had at this time, and ISPs generally retain their logs only for relatively brief periods of time. Without expedited discovery (i.e., discovery before a Rule 26(f) conference), Plaintiff will not be able to obtain the true identities of the infringers and obtain redress for the infringements. Nicolini Declaration, par. 7-8, 18-20, 22-24.

This problem, of course, is not unique to the Plaintiff in this case.

"[S]ituations arise, such as the present, where the identity of alleged defendants will not be known prior to the filing of a complaint. In such circumstances, the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds."

Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980).

The Internet has allowed the problem to worsen.

"With the rise of the Internet has come the ability to commit certain tortious acts, such as defamation, copyright infringement, and trademark infringement, entirely on-line. The tortfeasor can act pseudonymously or anonymously and may give fictitious or incomplete identifying information. Parties who have been injured by these acts are likely to find themselves chasing the tortfeasor from Internet Service Provider (ISP) to ISP, with little or no hope of actually discovering the identity of the tortfeasor. In such cases the traditional reluctance for permitting filings against John

1 Doe defendants or fictitious names and the traditional enforcement of strict
2 compliance with service requirements should be tempered by the need to provide
injured parties with an forum in which they may seek redress for grievances."

3 Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 577 (N.D. Cal. 1999).

4 As set forth in Semitool, Inc. v. Tokyo Electron Am., Inc., 208 F.R.D. 273, 276 (N.D.
5 Cal. 2002), the conventional standard of good cause is used in evaluating a request for expedited
6 discovery. Semitool explained further,

7 "Good cause may be found where the need for expedited discovery, in consideration
8 of the administration of justice, outweighs the prejudice to the responding party. It
should be noted that courts have recognized that good cause is frequently found in
9 cases involving claims of infringement and unfair competition."

10 See, also, Yokohama Tire Corp. v. Dealers Tire Supply, Inc., 202 F.R.D. 612, 613-14 (D. Ariz.
11 2001).

12 The burden of responding to subpoenas must be borne by all in the normal course of
13 administering justice. Without the expedited discovery, Plaintiff will be prejudiced to the extent
14 of foreclosing its ability to obtain redress for infringement of its copyrights. Further, although
15 not necessary to this analysis, copyright infringement is presumed to cause irreparable harm.
16 Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1254 (3d Cir. 1983).

17 When the identity of defendants is not known before a complaint is filed, a plaintiff
18 "should be given an opportunity through discovery to identify the unknown defendants, unless it
19 is clear that discovery would not uncover the identities, or that the complaint would be dismissed
20 on other grounds." Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980). In evaluating
21 whether a plaintiff establishes good cause to learn the identity of Doe defendants through early
22 discovery, courts examine whether the plaintiff (1) identifies the Doe defendant with sufficient
23 specificity that the court can determine that the defendant is a real person who can be sued in
24 federal court, (2) recounts the steps taken to locate and identify the defendant, (3) demonstrates
25 that the action can withstand a motion to dismiss, and (4) proves that the discovery is likely to
26 lead to identifying information that will permit service of process. Columbia Ins. Co. v.
27 Seescandy.com, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999).

1 Plaintiff has sufficiently specified the identity of each Defendant by the unique IP address
 2 and Timestamp associated with that Defendant when the Defendant committed infringement of
 3 Plaintiff's copyrighted Work, as set forth in **Exhibit A**. Nicolini Decl., par. 18.

4 Plaintiff has done all it could do to identify the Defendants by obtaining with respect to
 5 each Defendant the IP address, the Timestamp and the identity of the ISP. Thus, the necessity of
 6 conducting discovery through subpoenas. Nicolini Decl., par. 18-20.

7 As noted above, Plaintiff alleges in its Complaint that (i) it owns the copyright in the
 8 Work and the copyright registration covering the work, and that (ii) each Defendant listed in
 9 **Exhibit A** has, without permission or consent of Plaintiff, reproduced and distributed to the
 10 public at least a substantial portion of Plaintiff's copyrighted Work. Plaintiff has pled the
 11 essential elements to state a claim for copyright infringement against the Doe defendants under
 12 17 U.S.C. § 106(1) and (3) that would withstand a motion to dismiss. In addition, CEG has
 13 confirmed that the Defendants listed in Exhibit A infringed the copyright in the Work. Nicolini
 14 Decl., par. 17, 18 and 22.

15 The requested discovery by subpoena is necessary for Plaintiff to determine the true
 16 name and address of the individuals who performed the infringing acts. All concerns to avoid
 17 abuse are satisfied in this case.

18 B. The Discovery Sought by Plaintiff Is Reasonably Likely to
 19 Lead to Identifying Information About Defendant That
Would Make Service of Process Possible

20 The court in Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 580 (N.D. Cal. 1999),
 21 citing Gillespie v. Civiletti, 629 F.2d 637, 642 (9th Cir. 1980), ruled that a plaintiff should show
 22 that the discovery it seeks will be reasonably likely to lead to identifying information about
 23 defendants that would make service of process possible. As explained above, ISPs have logs and
 24 records that will link the IP address/Timestamp combination with a subscriber's name, address,
 25 telephone number and email address. With that information, Plaintiff will have sufficient
 26 information to name Defendants for purposes of issuing a summonses and making reasonable
 27 attempts to serve them.

C. Neither First Amendment Nor Privacy Rights Preclude Discovery

1. First Amendment Rights Are Not Abrogated Here

Plaintiff recognizes that there may be concern regarding First Amendment-free speech or privacy issues. The right of free speech is no more implicated in this case than in a case in which someone uses a DVD recorder to make and distribute to others copies of a motion picture. The Constitution itself, at Article I, Section 8, Clause 8, empowers Congress to providing for an author's exclusive rights to his works.

While First Amendment-free speech rights extend to anonymous speech on the Internet,

"Anonymous speech, like speech from identifiable sources, does not have absolute protection. The First Amendment, for example, does not protect copyright infringement, and the Supreme Court, accordingly, has rejected First Amendment challenges to copyright infringement actions. See, e.g., *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 555-56, 569, 105 S.Ct. 2218, 85 L.Ed.2d 588 (1985); *Universal City Studios, Inc. v. Reimerdes*, 82 F.Supp.2d 211, 220 (S.D.N.Y.2000) (the "Supreme Court ... has made it unmistakably clear that the First Amendment does not shield copyright infringement"). Parties may not use the First Amendment to encroach upon the intellectual property rights of others. See *In re Capital Cities/ABC, Inc.*, 918 F.2d 140, 143 (11th Cir. 1990)."

Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp. 2d 556, 562-63 (S.D.N.Y. 2004).

While a person who uses the Internet to download or distribute copyrighted works without permission may be engaging in speech, that person is engaging in speech only to a limited extent, and the First Amendment does not protect the person's identity from disclosure. Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp. 2d 556, 558 (S.D.N.Y. 2004).

2. Privacy Rights Are Not Abrogated Here

(a) There Is No Reasonable Expectation of Privacy Here

With respect to a purported right of privacy, the Defendants have little expectation of privacy because they opened their computers to others through peer-to-peer file sharing. See, e.g., UMG Recordings, Inc. v. Does 1-4, No. 06-0652 SBA, 2006 U.S. Dist. LEXIS 32821 at *8-9 (N.D. Cal. Mar. 6, 2006).

(b) 47 U.S.C. § 551 Does Not Preclude Compliance With the Subpoenas

Some ISPs may assert that the Cable Communications Policy Act of 1984, 47 U.S.C. § 551, prohibits disclosure of subscriber identities without the prior written or electronic consent of

the subscriber or a court order. They would be wrong since the names and addresses of such subscribers may be disclosed if the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure. 47 U.S.C. § 551(c)(2)(B) provides as follows:

"(c) Disclosure of personally identifiable information

"(2) A cable operator may disclose such information if the disclosure is—

"(B) subject to subsection (h) [relating to disclosures to governmental agencies] of this section, made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed"

In the order proposed by Plaintiff, provision is made for ISP's to given notice of the order.

Therefore, Plaintiff requests that the Court include in its order a statement that its order and the subpoena are appropriate under 47 U.S.C. § 551.

3. Joinder of Defendants Is Appropriate, and, Even If in Doubt, Should Not Be a Bar to the Discovery Sought at This Stage of Litigation

In cases throughout the country, copyright pirates have attempted to thwart discovery of their identities by asserting purported misjoinder in motions to quash subpoenas. Plaintiff contends that joinder is appropriate in this case. However, Plaintiff asserts also that the matter of joinder is not appropriately considered a bar to discovery at this stage of litigation.

With respect to joinder, the controlling rule is Fed. R. Civ. P. 20. It states in pertinent part,

Rule 20. Permissive Joinder of Parties

(a) Persons Who May Join or Be Joined.

(2) Defendants.

Persons * * * may be joined in one action as defendants if:

(A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out of the same transaction,

occurrence, or series of transactions or occurrences; and

(B) any question of law or fact common to all defendants will arise in the action.

(3) Extent of Relief.

Neither a plaintiff nor a defendant need be interested in obtaining or defending against all the relief demanded. The court may grant judgment to one or more plaintiffs according to their rights, and against one or more defendants according to their liabilities.

(b) Protective Measures.

The court may issue orders — including an order for separate trials — to protect a party against embarrassment, delay, expense, or other prejudice that arises from

1 including a person against whom the party asserts no claim and who asserts no
2 claim against the party.

3 "Under the Rules, the impulse is toward entertaining the broadest possible scope of action
4 consistent with fairness to the parties; joinder of claims, parties and remedies is strongly
5 encouraged." United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 724 (1966).

6 In this case, Plaintiff alleges that all the Doe defendants have engaged in the same
7 transaction, occurrence, or series of transactions or occurrences, namely, that each of the Doe
8 defendants has infringed the same copyrighted work, and that they did so using the same scheme,
9 namely using a BitTorrent P2P network, in cooperation with each other. Complaint, par. 10.
10 Plaintiff further alleges that the Doe defendants have cooperated with each other. Complaint,
11 par. 11. The allegations are supported by the Nicolini Declaration (Doc. #30). See, for example,
12 par. 22 of the Nicolini Declaration wherein Mr. Nicolini testifies, among other things, (emphasis
13 added):

14 "the hashes associated with the torrent files on the computers having the IP
15 addresses and time stamps listed in Exhibit A are all identical to each other, that
16 is, **they all have the same hash. This demonstrates that all the Doe
17 defendants listed in Exhibit A joined the same swarm.**"

18 In addition, according to BitTorrent, Inc. itself, the very purpose of the BitTorrent
19 protocol is to allow people to **both** download a file and for them to upload what they had
20 downloaded to others. Nicolini Decl., par. 7.

21 With respect to the duration of a swarm (and concomitantly, the period of time in which
22 Defendants can participate in cooperative or joint activity) Mr. Nicolini declares in par. 6
23 (emphasis added),

24 "Persons seeking to download such a work also access the Internet through an ISP
25 (which may or may not be the same ISP as used by the original seeder) and seek
26 out the work on a P2P network. With the availability of the seed, other users,
27 who are referred to as "peers," access the Internet and request the file (by
28 searching for its title or even searching for the torrent's "hash" - described below)
and engage the original seeder and/or each other in a group, sometimes referred
to as a "swarm," and begin downloading the seed file. In turn, as each peer
receives portions of the seed, most often that peer makes those portions available
to other peers in the swarm. Therefore, each peer in the swarm is at least copying
and is usually distributing, as a follow-on seeder, copyrighted material at the same
time. Of the over 20,000 infringers tracked in connection with several cases
currently pending, at least 95% of the Doe defendants were uploading (i.e.,
distributing) illegal copies of our clients' motion pictures at the moment indicated

by the Timestamp in the respective Exhibit A appended to each complaint, which is also true for this case. In P2P networks, the infringement may continue even after the original seeder has gone completely offline. Any BitTorrent client may be used to join a swarm. **As more peers join a swarm at any one instant, they obtain the content at even greater speeds because of the increasing number of peers simultaneously offering the content as seeders themselves for unlawful distribution. As time goes on, the size of the swarm varies, yet it may endure for a long period, with some swarms enduring for 6 months to well over a year depending on the popularity of a particular motion picture.** As a result, the original seed file becomes unlawfully duplicated multiple times by multiple parties, with a potentially exponential increase in the number of illegal copies of any copyrighted work. With respect to any particular swarm, the hash (an alphanumeric representation of a digital file) associated with the copied file's torrent file remains the same."

The foregoing allegations also demonstrate that there are questions of law and fact common to all defendants that may arise in this action, including whether or not each defendant infringed the single copyright in suit.

In Call of the Wild, 770 F. Supp. 2d, at 344-345, Judge Howell discussed in detail why joinder, particularly at this stage of litigation, is proper in cases such as the instant case. Further consideration of joinder (or severance) at this stage of litigation could result in plaintiffs' being unable to protect their copyrights in a cost-effective manner (emphasis added):

"The plaintiffs, by contrast, are currently obtaining identifying information from ISPs so that they can properly name and serve the defendants. If the Court were to consider severance at this juncture, plaintiffs would face significant obstacles in their efforts to protect their copyrights from illegal file-sharers and this would only needlessly delay their cases. The plaintiffs would be forced to file 5,583 separate lawsuits, in which they would then move to issue separate subpoenas to ISPs for each defendant's identifying information. Plaintiffs would additionally be forced to pay the Court separate filing fees in each of these cases, which would further limit their ability to protect their legal rights. This would certainly not be in the 'interests of convenience and judicial economy,' or 'secure a just, speedy, and inexpensive determination of the action.' *Lane*, 2007 WL 2007493, at *7 (declining to sever defendants where 'parties joined for the time being promotes more efficient case management and discovery' and no party prejudiced by joinder).

"Given the administrative burden of simply obtaining sufficient identifying information to properly name and serve alleged infringers, it is highly unlikely that the plaintiffs could protect their copyrights in a cost-effective manner. Indeed, Time Warner urges the Court to sever the defendants for this very reason. Time Warner asserts that, if joinder were disallowed, its burden of complying with subpoenas would be diminished because the plaintiffs would not be able to proceed against all of the putative defendants individually. See Transcript of Mot. Hearing, 14-16, Call of the Wild Movie LLC v. Does 1-1,063, No. 10-cv-455 (Mar. 1, 2011).

"At this procedural juncture, the plaintiffs have met the requirements of permissive joinder under Rule 20(a)(2). The putative defendants are not prejudiced but likely benefited by joinder, and severance would debilitate the plaintiffs'

efforts to protect their copyrighted materials and seek redress from the putative defendants who have allegedly engaged in infringing activity. Courts are instructed to "entertain[] the broadest possible scope of action consistent with fairness to the parties." *Lane*, 2007 WL 2007493, at *7. **While this Court is fully cognizant of the logistical and administrative challenges of managing a case with numerous putative defendants, a number of whom may seek to file papers *pro se*, severing the putative defendants is no solution to ease the administrative burden of the cases. The Court therefore declines to sever the putative defendants at this time.**"

Magistrate Judges of this District issued early discovery orders in cases similar to the instant case while noting the joinder issue.³ In the Order issued by Chief Magistrate Judge Maria-Elena James on April 18, 2011 in Case No. CV 10-05863 MEJ, Document # 8, and in the Order issued by Magistrate Judge Joseph C. Spero on May 9, 2011 in Case No. CV 10-05885 JCS, Document # 13, both specifically noted with respect to the joinder issue (emphasis added),

"joinder of all defendants at this stage of the litigation is proper. This decision is without prejudice to any motion for severance by a current Doe defendant who is later included in this action by his or her true name."

Typically these copyright pirates rely on, and intentionally miss the point of,

BMG Music v. Does, No. C 06-01579, 2006 U.S. Dist. LEXIS 53237 (N.D. Cal. Jul. 31, 2006);
Twentieth Century Fox Film Corp. v. Does 1-12, No. C 04-04862 WHA (N.D. Cal. Nov. 16, 2004);
LaFace Records, LLC v. Does 1-38, No. 5:07-cv-298, 2008 WL 544992, 2008 U.S. Dist. LEXIS 14544 (E.D. N.C. Feb. 27, 2008); and
Interscope Records v. Does 1-25, No. 6:04-cv-197, 2004 U.S. Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004).

The plaintiffs in each of those case failed to contend that the Doe defendants acted in concert with each other.

In BMG Music v. Does, 2006 U.S. Dist. LEXIS 53237, at [*5-*6] Judge Marilyn Hall Patel explained the basis of her ruling and the ruling in the Twentieth Century Fox case (emphasis added):

"The only connection between defendants noted by plaintiffs' papers is the fact that defendants allegedly used the same ISP, Covad Communications, to conduct the infringing acts. Mot. at 2. However, absent any allegation that these individuals acted in concert, there is no basis for joinder.

³ The Hon. Magistrate Judge Grewal, in Diabolic Video Productions, Inc. v. Does 1-2099, CV 10-05865-PSG, Docket No. 16 (N.D. Cal. 2011), has been the exception. His ruling relied on an erroneous understanding of the four cases discussed below.

"Numerous federal courts have found that joinder is improper when **there is no allegation that multiple defendants acted in concert**. See Twentieth Century Fox Film Corp. v. Does 1-12, No. C 04-04862 WHA (N.D. Cal. Nov. 16, 2004) (Alsup, J.) (severing multiple Doe defendants in a copyright infringement case where although defendants used the same ISP to allegedly infringe motion picture recordings, there was no allegation that the individuals acted in concert)"

In LaFace Records there were several plaintiffs enforcing several copyrights. "Plaintiffs are the alleged owners of the copyrights in numerous sound recordings made by artists who no longer control the copyrights at issue. * * * Attached to the complaint are charts showing * * * a list of copyrighted recordings downloaded by artist, song title, album title, and copyright holder." 2008 U.S. Dist. LEXIS 14544, at [*2-*3]. The court based its ruling on this: "courts have commonly held that **where there is no assertion that multiple defendants have acted in concert, joinder is improper**." 2008 U.S. Dist. LEXIS 14544, at [*7]. (Emphasis added.)

In Interscope Records v. Does 1-25, there were SIXTEEN plaintiffs enforcing DOZENS of different copyrighted songs. Magistrate Judge Baker ruled that "the various Plaintiffs' claims against various Defendants are not logically related to each other." 2004 U.S. Dist. LEXIS 27782, at [*6]. This was based on the following facts: "None of the Defendants disseminated the same copyrighted material or songs belonging to the same set of Plaintiffs," 2004 U.S. Dist. LEXIS 27782, at [*11] and "Sixteen unrelated Plaintiffs have joined twenty-five unrelated Defendants who independently copied different songs owned by different Plaintiffs." 2004 U.S. Dist. LEXIS 27782, at [*15].

In the instant case, there is only a SINGLE plaintiff enforcing a SINGLE copyright. So, there is no issue of unrelated plaintiffs, or even of a plaintiff trying to enforce unrelated copyrights. And, all the Doe defendants are related to each other. The following allegation is in paragraph 11 of the Complaint,

"Each Defendant has acted in cooperation with the other Defendants by agreeing to provide, and actually providing, on a P2P network an infringing reproduction of at least substantial portions of Plaintiff's copyrighted Motion Picture, in anticipation of the other Defendants doing likewise with respect to that work and/or other works."

This allegation is supported by the testimony in the Nicolini Declaration. As explained by Mr. Nicolini, the accused Doe Defendants act, and must act, cooperatively to distribute

1 unlawful copies of the copyrighted work, and "all the Doe defendants listed in **Exhibit A** joined
2 the same swarm." Nicolini Decl., pars. 7, 18, and 22.

3 While Plaintiff uses the phrase "in cooperation" as opposed to "in concert," those phrases
4 are synonymous. See, <http://www.merriam-webster.com/dictionary/cooperate>.

5 In another "swarm" copyright infringement case decided by Judge Howell, namely
6 Voltage Pictures, LLC v. Does 1-5000, 2011 U.S. Dist. LEXIS 50787 (D.D.C. May 12, 2011)⁴,
7 the court distinguishes the cases that ordered severance, and notes that BitTorrent file sharing
8 uses a "swarm" of infringers. In that case, the court denied motions to quash by several
9 defendants. Judge Howell explained, at 2011 U.S. Dist. LEXIS 50787, at [*35]-[*39], as follows
10 (emphasis added):

11 "Some courts in other jurisdictions have granted motions by putative
12 defendants for severance in analogous copyright infringement cases against
13 unknown users of peer-to-peer file-sharing programs for failure to meet the 'same
14 transaction or occurrence test' in Rule 20(a)(2). Those courts have been confronted
15 with bare allegations that putative defendants used the same peer-to-peer network
16 to infringe copyrighted works and found those allegations were insufficient for
17 joinder. See, e.g., IO Grp., Inc. v. Does 1-19, No. 10-03851, 2010 WL 5071605, at
18 *8-12 (N.D. Cal. Dec. 7, 2010); Arista Records, LLC v. Does 1-11, No. 07-cv-
19 2828, 2008 WL 4823160, at *6 (N.D. Ohio Nov. 3, 2008) ('merely alleging that the
20 Doe Defendants all used the same ISP and file-sharing network to conduct
21 copyright infringement without asserting that they acted in concert was not enough
22 to satisfy the same series of transactions requirement under the Federal Rules.');

23 LaFace Records, LLC v. Does 1-38, No. 5:07-cv-298, 2008 WL 544992, at *3
24 (E.D. N.C. Feb. 27, 2008) (severing putative defendants in file-sharing case not
25 involving BitTorrent technology, noting that 'other courts have commonly held that
26 where there is no assertion that multiple defendants have acted in concert, joinder
is improper.');

27 Interscope Records v. Does 1-25, No. 6:04-cv-197, 2004 U.S. Dist.
28 LEXIS 27782 (M.D. Fla. Apr. 1, 2004) (adopting Mag. J. Report and
Recommendation at Interscope Records v. Does 1-25, No. 6:04-cv-197, 2004 U.S.
Dist. LEXIS 27782 (M.D. Fla. Apr. 1, 2004)). That is not the case here.

"The plaintiff has provided detailed allegations about how the BitTorrent
technology differs from other peer-to-peer file-sharing programs and necessarily
engages many users simultaneously or sequentially to operate. See Columbia
Pictures Indus. v. Fung, No. 06-5578, 2009 U.S. Dist. LEXIS 122661, at *7 (C.D.
Cal. Dec. 21, 2009) (**BitTorrent 'is unique from that of previous [P2P] systems
such as Napster and Grokster. Rather than downloading a file from an
individual user, [BitTorrent users download] from a number of host
computers that possess the file simultaneously. . . . The BitTorrent client
application simultaneously downloads the pieces of the content file from as
many users as are available at the time of the request, and then reassembles
the content file on the requesting computer when the download is complete.**

4 This case, too, was cited with approval in MCGIP, LLC v. Does 1-18, 2011 U.S. Dist.
LEXIS 64188 [*1, *3] (N.D. Cal. June 2, 2011), by United States District Judge Edward M.
Chen.

1 **Once a user downloads a given content file, he also becomes a source for**
 2 **future requests and downloads.').** Specifically, BitTorrent creates a 'swarm' in
 3 which 'each additional user becomes a part of the network from where the file can
 4 be downloaded . . . [U]nlike a traditional peer-to-peer network, each new file
 5 downloader is receiving a different piece of the data from each user who has
 6 already downloaded the file that together comprises the whole.' Second Am.
 7 Compl., ¶ 3.

8 "At least one court has not been persuaded that allegations of copyright
 9 infringement by users of BitTorrent satisfy the requirement of Rule 20. See, e.g.,
 10 Lightspeed v. Does 1-1000, No. 10-cv-5604, 2011 U.S. Dist. LEXIS 35392, at *4-
 11 7 (N.D. Ill. Mar. 31, 2011) (finding that Doe defendants using BitTorrent
 12 technology were misjoined on the basis that the putative defendants were not
 13 involved in the 'same transaction, occurrence, or series of transactions or
 14 occurrence' under FED. R. CIV. P. 20(a)(2)(A)); Millennium TGA Inc. v. Does 1-
 15 800, No. 10-cv-5603, 2011 U.S. Dist. LEXIS 35406, at *3-5 (N.D. Ill. Mar. 31,
 16 2011) (same). In those cases, the court did not discuss the precise nature of the
 17 BitTorrent technology, which enables users to contribute to each other's infringing
 18 activity of the same work as part of a 'swarm.' In any event, by contrast to the
 19 instant claim of infringement of a single copyrighted work by the putative
 20 defendants, the plaintiffs in Lightspeed and Millennium TGA Inc. alleged
 21 infringement of multiple works, a factor that may undermine the requisite
 22 showing of concerted activity to support joinder.

23 Here, as in Voltage Pictures, Plaintiff alleges that the Doe defendants have acted in
 24 cooperation with each other (i.e., in concert), and Plaintiff's expert, Nicolini, explained (here par.
 25 6 and a portion of par. 22 are repeated for convenience, with emphasis added),

26 "P2P networks distribute infringing copies of motion pictures (and works in other
 27 forms such as music and books) with file sharing software such as BitTorrent as
 28 follows: The process begins with one user accessing the Internet through an
 29 Internet Service Provider ('ISP') and intentionally making a digital file of the work
 30 available on the Internet to the public from his or her computer. This first file is
 31 often referred to as the first 'seed.' I will refer to the person making this seed
 32 available as the 'original seeder.' Persons seeking to download such a work also
 33 access the Internet through an ISP (which may or may not be the same ISP as
 34 used by the original seeder) and seek out the work on a P2P network. With the
 35 availability of the seed, other users, who are referred to as 'peers,' access the
 36 Internet and request the file (by searching for its title or even searching for the
 37 torrent's 'hash' - described below) and engage the original seeder and/or each
 38 other in a group, sometimes referred to as a 'swarm,' and begin downloading the
 39 seed file. In turn, as each peer receives portions of the seed, most often that peer
 40 makes those portions available to other peers in the swarm. Therefore, each peer
 41 in the swarm is at least copying and is usually distributing, as a follow-on seeder,
 42 copyrighted material at the same time. Of the over 20,000 infringers tracked in
 43 connection with several cases currently pending, at least 95% of the Doe
 44 defendants were uploading (i.e., distributing) illegal copies of our clients' motion
 45 pictures at the moment indicated by the Timestamp in the respective Exhibit A
 46 appended to each complaint, which is also true for this case. In P2P networks, the
 47 infringement may continue even after the original seeder has gone completely
 48 offline. Any BitTorrent client may be used to join a swarm. As more peers join a
 49 swarm at any one instant, they obtain the content at even greater speeds because
 50 of the increasing number of peers simultaneously offering the content as seeders

1 themselves for unlawful distribution. As time goes on, the size of the swarm
 2 varies, yet it may endure for a long period, with some swarms enduring for 6
 3 months to well over a year depending on the popularity of a particular motion
 4 picture. As a result, the original seed file becomes unlawfully duplicated multiple
 5 times by multiple parties, with a potentially exponential increase in the number of
 6 illegal copies of any copyrighted work. **With respect to any particular swarm,**
 7 **the hash (an alphanumeric representation of a digital file) associated with the**
 8 **copied file's torrent file remains the same.**

9 ***

10 "... the hashes associated with the torrent files on the computers having the
 11 IP addresses and time stamps listed in Exhibit A are all identical to each
 12 other, that is, they all have the same hash. This demonstrates that all the Doe
 13 defendants listed in Exhibit A joined the same swarm."

14 This evidence establishes that the Doe defendants are properly joined. This particular
 15 issue was specifically addressed by Magistrate Judge Elizabeth D. Laporte in Hard Drive
 16 Productions v. Does 1-42, N.D. Cal. Case No. CV 11-01956 EDL (N.D. Cal. Decided August 3,
 17 2011) Doc. #20 (emphasis added):

18 "This Court [originally] denied the application [for early discovery] without
 19 prejudice due to an inadequate showing that the Defendants were properly joined.
 20 Plaintiff subsequently filed a Revised Application on June 16, 2011 with an
 21 extended discussion on joinder.

22 "On July 14, 2011, this Court again denied the application without
 23 prejudice because Plaintiff did not make a sufficient showing that the Doe
 24 Defendants were participating in a common BitTorrent swarm and a leave was
 25 granted for Plaintiff to submit a declaration to remedy the deficiency. **Plaintiff**
 26 **then filed its Supplemental Declaration of Peter Hansmeier, confirming that**
 27 **all the Doe Defendants participated in a common swarm because the torrent**
 28 **file shared among the swarm was identified by a unique file hash.** Hansmeier
 Supp. Decl. [Doc. #18], ¶ 5.

"Having considered Plaintiff's Supplemental Declaration of Peter
 Hansmeier as well as Plaintiff's prior submissions, the Court hereby GRANTS
 Plaintiff's Revised Ex Parte Application on the grounds that Plaintiff has
 demonstrated good cause to take early discovery. Plaintiff has met the burden of
 showing that the information requested by the discovery was necessary to effect
 service on the Doe Defendants, as well as demonstrating a basis for joining the
 Doe Defendants in this action."

In MCGIP, LLC v. Does 1-18, 2011 U.S. Dist. LEXIS 64188 [*2] (N.D. Cal. June 2,
 2011), United States District Judge Edward M. Chen held:

Fourth, Doe's assertion of improper joinder may be meritorious but, '[a]t this
 stage in the litigation, . . . when discovery is underway [only] to learn identifying
 facts necessary to permit service on Doe defendants, joinder . . . of unknown
 parties identified only by IP addresses is proper,' particularly where, are here, the
 complaint contains allegations that the Doe Defendants have infringed Plaintiff's
 copyright through 'the same file-sharing software program [i.e., BitTorrent] that
 operates through simultaneous and sequential computer connections and data

transfers among the users.' *Voltage*, 2011 U.S. Dist. LEXIS 50787, at *29. Doe may, at a later point in this litigation, raise the joinder issue if Plaintiff maintains this action against him or her.

So, joinder is proper in this case, particularly at this stage of litigation.

4. Consideration of the Personal Jurisdiction Issue at this Stage of Litigation Is Premature

Copyright pirates have also attempted to thwart discovery of their identities by asserting purported lack of personal jurisdiction in motions to quash subpoenas. However, a purported absence of personal jurisdiction over a potential defendant is NOT a competent basis for quashing a subpoena.

Rule 45(c) of the Federal Rules of Civil Procedure provides as follows relating to quashing a subpoena:

(3) Quashing or Modifying a Subpoena.

(A) When Required. On timely motion, the issuing court must quash or modify a subpoena that:

- (i) fails to allow a reasonable time to comply;
- (ii) requires a person who is neither a party nor a party's officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person — except that, subject to Rule 45(c)(3)(B)(iii), the person may be commanded to attend a trial by traveling from any such place within the state where the trial is held;
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
- (iv) subjects a person to undue burden.

(B) When Permitted. To protect a person subject to or affected by a subpoena, the issuing court may, on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information;
- (ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party; or
- (iii) a person who is neither a party nor a party's officer to incur substantial expense to travel more than 100 miles to attend trial.

(C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(c)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

1 A potential defendant is not required to do anything by the subpoena. An ISP is required
2 to do something, but not a potential defendant. Even if a potential defendant travels not a foot,
3 produces not one record or answers no questions, he or she would not be held in non-compliance
4 with the subpoena. So, Rule 45(c)(3)(A) provides no basis for quashing the subpoena.

5 A potential defendant might contend that he is a person affected by the subpoena. But
6 that is not sufficient to quash a subpoena. Rule 45(c)(3)(B) allows a court to quash a subpoena
7 only if (i) trade secret or other confidential research, development, or commercial information
8 would be disclosed – and his name and identifying information are not such information; (ii)
9 certain expert opinion or information would be disclosed – and no expert opinion or information
10 is being sought, and (iii) a person in the position of a non-party, would be required to travel more
11 than 100 miles to attend trial – and that is not at issue here.

12 Plaintiff notes that Rule 45(c)(3)(C) provides that in any event the Court may require
13 production pursuant to the subpoena if Plaintiff shows substantial need for the requested
14 material. Plaintiff has already done so herein.

15 It follows that consideration of personal jurisdiction (just as with joinder/severance) is
16 improper under the guise of trying to quash a subpoena.

17 Further in this regard, at this stage of the litigation, when no defendants have actually
18 been named to this lawsuit, personal jurisdiction consideration is premature. Once Plaintiff has
19 actually named defendants and has an opportunity to challenge, by discovery, any jurisdictional
20 contentions made by a named defendant, then, at that time, personal jurisdiction may be
21 considered.

22 In Sony Music Entertainment Inc. v. Does 1-40, 326 F.Supp.2d 556, 567 (S.D.N.Y.
23 2004), the court noted:

24 "[W]ithout the identifying information sought by plaintiffs in the Cablevision
25 subpoena, it would be difficult to assess properly the existence of personal
26 jurisdiction over the Doe defendants. This analysis requires an evaluation of the
27 contacts between the various defendants and the forum state. A holding at this
28 stage that personal jurisdiction is lacking would be premature."

(Footnote and citations omitted.)

1 Call of the Wild Movie is directly on point and well-reasoned. Judge Howell, at p. 347-8,
 2 specifically held that consideration of the personal jurisdiction issue is premature at this stage of
 3 litigation. Judge Howell's analysis is directly analogous and applicable to the situation here
 4 (Emphasis added).

5 "The Court rejects this argument [that it lacks personal jurisdiction] for
 6 three reasons. First, as the Amici concede, publicly available IP lookups reveal
 7 only where a defendant is 'likely' to be located. *Id.* at ¶ 4. Given that these lookup
 8 tools are not completely accurate, this does not resolve the question of whether
 9 personal jurisdiction would be proper. Ultimately, the Court would still be unable
 10 to properly evaluate jurisdictional arguments until the putative defendants are
 properly identified and named. *See Sony*, 326 F. Supp. 2d. at 567-68 ('Assuming
 personal jurisdiction were proper to consider at this juncture, the [publicly
 available IP lookup] techniques suggested by amici, at best, suggest the mere
 'likelihood' that a number of defendants are located [outside this jurisdiction].
 This, however, does not resolve whether personal jurisdiction would be proper.').

11 "Second, **the nature of the BitTorrent technology enables every user of**
 12 **the file-sharing protocol to access copyrighted material from other peers,**
 13 **who may be located in multiple jurisdictions 'around the country,' including**
 14 **this one.** Amended Compl., *Wild*, ECF No. 6, ¶ 4. Amici raise the prospect that
 15 the consequence of this theory is that any Internet user may be haled into court in
 16 any jurisdiction in the country for any online activity. Transcript of Mot. Hearing
 17 at 34-35, *Call of the Wild Movie LLC v. Does 1-1,063*, No. 10-cv-455 (Mar. 1,
 18 2011) ('If merely placing information online were enough to establish personal
 19 jurisdiction in the District or anyplace their information could be obtained and
 20 downloaded and accessed, the limits on personal jurisdiction would be
 abolished.'). While that broad prospect would indeed be troubling, that is not the
 situation here. *See generally GTE New Media Servs.*, 199 F.3d at 1350 ('[T]he
 advent of advanced technology, say, as with the Internet, should [not] vitiate long-
 held and inviolate principles of federal court jurisdiction.'). **The allegations in the**
Complaints in *Wild*, *Maverick* and *Donkeyball* do not involve general Internet
access, but specific use of a file-sharing protocol that may touch multiple
jurisdictions to effectuate a download of a single copyrighted work.
Moreover, so far, no putative defendant has been named or 'haled' before
this Court. The plaintiffs in each case will be able to proceed only against
those named defendants over whom this Court has personal jurisdiction.

21 "Finally, at this juncture when no putative defendant has been named, the
 22 Court has limited information to assess whether any putative defendant has a
 23 viable defense of lack of personal jurisdiction or to evaluate possible alternate
 24 bases to establish jurisdiction. *See, e.g., London-Sire Records, Inc.*, 542 F. Supp.
 25 2d at 181 ('Even taking all of the facts in [the putative defendant's] affidavit as
 26 true, it is possible that the Court properly has personal jurisdiction.'); *Humane*
 27 *Soc'y of the United States v. Amazon.com, Inc.*, No. 07-623, 2007 U.S. Dist.
 28 LEXIS 31810, at *10 (D.D.C. May 1, 2007) ('[A] plaintiff faced with a motion to
 dismiss for lack of personal jurisdiction is entitled to reasonable discovery, lest
 the defendant defeat the jurisdiction of a federal court by withholding information
 on its contacts with the forum,' quoting *Virgin Records Am., Inc. v. Does 1-35*,
 No. 05-1918, 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006)). Certainly, the
 Court concurs with Amici that the putative defendants deserve to have dispositive
 issues, such as personal jurisdiction, decided promptly. Amici Reply Brief, *Wild*,
 ECF No. 22, at 10. **When the defendants are named, they will have the**
opportunity to file appropriate motions challenging the Court's jurisdiction

and that will be the appropriate time to consider this issue. *See Virgin Records*, 2006 WL 1028956, at *3 (Amici's personal jurisdiction arguments rejected since 'Defendant's Motion to Quash is without merit [] because it is premature to consider the question of personal jurisdiction in the context of a subpoena directed at determining the identity of the Defendant,' citing *Elektra Entm't Grp., Inc. v. Does 1-9*, No. 04-2289, 2004 WL 2095581, at *5 (S.D.N.Y. Sept. 8, 2004); *Sony*, 326 F. Supp. 2d 556, 567-68 (S.D.N.Y.2004); *UMG Recordings v. Does 1-199*, No. 04-0093, at *2 (D.D.C. Mar. 10, 2004)).

"The Court and parties are in no position yet to evaluate each putative defendant's specific connection with this jurisdiction. Quashing the subpoenas would effectively bar the plaintiffs' from obtaining discovery pertinent to that evaluation, and **this Court declines to cut off jurisdictional discovery prematurely.**"

Even if an purported defendant were to declare under penalty of perjury that he has no contacts within this jurisdiction, **a court should not put any credence in such statements at this stage of the litigation**, when Plaintiff has had no opportunity to test, through discovery, their truthfulness.

In this regard, the Court is asked to take notice that we have recently experienced a week of a U.S. Congress member's making untrue statements and partial answers all in the name of protecting privacy and preventing embarrassment. He falsely claimed several times that a particular a message was sent by a hacker and not by himself, even though in making such false claim he effectively impugned the security measures against hacking by Twitter and other Internet services. **The Congressman did not become forthright until additional information was discovered.** See the story here, e.g.,

<http://www.businessweek.com/news/2011-06-07/weiner-apologizes-for-photos-that-imperil-his-political-future.html>.

In Voltage Pictures, Judge Howell refused to consider motions to dismiss at this stage of litigation, even though many of the Doe defendants names and addresses were known to the plaintiff. In Voltage Pictures, at p. 21-22, Judge Howell further explained (footnotes omitted, emphasis added),

"Although the putative defendants assert that they do not have sufficient contacts with this jurisdiction to justify personal jurisdiction, the Court, as well as the plaintiff, has limited information to assess whether these jurisdictional defenses are valid and to evaluate possible alternate bases to establish jurisdiction. *See, e.g., London-Sire Records, Inc.*, 542 F. Supp. 2d at 181 ('Even taking all of the facts in [the putative defendant's] affidavit as true, it is possible that the Court properly has personal jurisdiction.');

Humane Soc'y of the United States v.

Amazon.com, Inc., No. 07-623, 2007 U.S. Dist. LEXIS 31810, at *10 (D.D.C. May 1, 2007) ('[A] plaintiff faced with a motion to dismiss for lack of personal jurisdiction is entitled to reasonable discovery, lest the defendant defeat the jurisdiction of a federal court by withholding information on its contacts with the forum,' quoting *Virgin Records Am., Inc. v. Does I-35*, No. 05-1918, 2006 WL 1028956, at *3 (D.D.C. Apr. 18, 2006)). To be clear, at this stage in the proceedings, the plaintiff is engaged in discovery to identify the proper defendants to be named in this lawsuit, including whether the exercise of jurisdiction over each potential defendant is proper. **If and when the putative defendants are ultimately named in this lawsuit, the defendants will have the opportunity to file appropriate motions challenging the Court's jurisdiction, and the Court will be able to evaluate personal jurisdiction defenses and consider dismissal. Until that time, however, dismissal under Rule 12(b)(2) is inappropriate.** See *London-Sire Records*, 542 F. Supp. 2d at 180-181 ('premature to adjudicate personal jurisdiction' and permitting plaintiff to engage in jurisdictional discovery); *Sony*, 326 F. Supp. 2d at 567-68 (same); *Virgin Records*, 2006 WL 1028956, at *3 ('Defendant's Motion to Quash is without merit [] because it is premature to consider the question of personal jurisdiction in the context of a subpoena directed at determining the identity of the Defendant,' citing *Elektra Entm't Grp., Inc. v. Does I-9*, No. 04-2289, 2004 WL 2095581, at *5 (S.D.N.Y. Sept. 8, 2004); *UMG Recordings v. Does I-199*, No. 04-0093, slip op. at 2 (D.D.C. Mar. 10, 2004)). **Accordingly, the putative defendants' motions to dismiss based on a purported lack of personal jurisdiction are denied at this time.**

Like the putative defendants in *Voltage Pictures*, **"if and when putative defendant" Doe X is "ultimately named in this lawsuit," putative defendant Doe X "will have the opportunity to file appropriate motions challenging the Court's jurisdiction"**

Further, with copyright infringement involving cooperation with many potential defendants in this District (Nicolini Decl., par. 23), or having a direct effect on Plaintiff in California, this Court may exercise personal jurisdiction over out-of-state defendants under the effects test set out in *Calder v. Jones*, 465 U.S. 783, 79 L. Ed. 2d 804, 104 S. Ct. 1482 (1984). As explained by U.S. District Judge Patel in *IO Group, Inc. v. Pivotal*, No. C 03-5286 MHP, 2004 U.S. Dist. LEXIS 6673, 2004 WL 838164, *6 (N.D. Cal. Apr. 19, 2004),

"Finally, this court may also exercise specific jurisdiction over defendants under the *Calder* effects test. See *Panavision v. Int'l, LP v. Toeppen*, 141 F.3d 1316, 1321 (9th Cir. 1998) (citing *Calder v. Jones*, 465 U.S. 783, 79 L. Ed. 2d 804, 104 S. Ct. 1482 (1984)). [*17] Under *Calder*, personal jurisdiction can be based upon '(1) intentional actions, (2) expressly aimed at the forum state, (3) causing harm, the brunt of which is suffered--and which the defendant knows would likely be suffered--in the forum state.' *Id.* (citing *Core-Vent Corp. v. Nobel Ind. AB*, 11 F.3d 1482, 1486 (9th Cir. 1993)). Copyright infringement may be characterized as an intentional tort. See *Columbia Pictures Television v. Krypton Broad. of Birmingham, Inc.*, 106 F.3d 284, 289 (9th Cir. 1997), overruled on other grounds by *Feltner v. Columbia Pictures Television*, 523 U.S. 340, 140 L. Ed. 2d 438, 118 S. Ct. 1279 (1998);

"* * * IO Group also alleges that all of the studios in the gay adult entertainment industry are located in California. Webb Decl. P21. As a result, defendants knew that the brunt of the harm resulting from their infringement would likely be felt in California. Based on this evidence, IO Group has adequately demonstrated that defendants published images belonging to a California company, affecting an industry primarily centered in California, knowing that harm would likely be felt in that state. Construing these facts in a light most favorable to the plaintiff, IO Group has made a prima facie case that defendants are subject to the personal jurisdiction of this court under *Calder*."

Thanks to, among other reports, a CBS "60 Minutes" report, Americans have long known that California is the center of adult motion picture production. See,

<http://www.cbsnews.com/stories/2003/11/21/60minutes/main585049.shtml>

D. The Exemplary Subpoena Will Elicit the Required Information

Plaintiff requests that the Court issue an order allowing Plaintiff to immediately serve (i.e., before a Rule 26(f) conference) a subpoena on each of the ISPs listed in **Exhibit A** in substantially the same form as the example attached hereto as **Exhibit 1**. The example subpoena identifies an ISP as the recipient of the subpoena, and requests that the recipient produce,

"Documents sufficient to identify the names, addresses, telephone numbers, and e-mail addresses of [ISP's] subscribers assigned the IP addresses identified on Attachment A on the corresponding dates at the corresponding times. You are to comply with this subpoena pursuant to the terms set forth in the Order attached hereto as Attachment B."

Attachment A is a sample of a list, that would be compiled from **Exhibit A**, of Doe Defendants with IP addresses and Timestamps corresponding to the ISP to be served with the subpoena. Attachment B will be the order as signed by the Court.

The information sought by the subpoena will be sufficient to enable Plaintiff to identify the Doe Defendants and facilitate service of process.

IV. **THERE IS NO NEED FOR TENDERING WITNESS AND MILEAGE FEES**

The subpoenas to be issued will be only for production of documents and records. No appearance at a deposition will be required.

Rule 45(b)(1) provides (with emphasis added):

"Service of a subpoena upon a person named therein shall be made by delivering a copy thereof to such person and, **if the person's attendance is commanded**, by tendering to that person the fees for one day's attendance and the mileage allowed by law."

However, Rule 45(c)(2)(A) provides (with emphasis added):

"Appearance Not Required. A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, **need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.**"

In Martindale v. Windsor, 75 F.R.D. 665, 670 (D. Colo. 1997), third party witnesses, who were only required to produce documents, sought to quash subpoenas on the ground that witness and mileage fees had not been tendered. The court declined to do so, ruling that such fees are not required where production, but no appearance, is required by a subpoena:

"Plaintiff's response to the issue of witness fees is to argue that he was not requesting an appearance of either individual, only production of the documents. In this case, Marr and Kurtz are both employed at AVCF. They were both served at AVCF. Therefore, no mileage would be appropriate and no requirement was made that either individual appear for a deposition. They only had to produce the documents. Both argue that '[b]asically, this is a records deposition ...' Motion to Quash, p. 3. The subpoena compels nothing more than production of the documents. There was no need to attend any deposition. In this case, there was no requirement that a witness fee and mileage be tendered along with the subpoena."

To avoid confusion in the event that an ISP insists upon advance payment of witness and mileage fees, Plaintiff requests that the Court's order specify that witness and mileage fees required by Rule 45(b)(1) of the Federal Rules of Civil Procedure do not apply. The Proposed Order includes provisions in this regard.

V. CONCLUSION

In view of the foregoing, Plaintiff respectfully requests that its Ex Parte Application be granted and that the Court enter an order substantially in the form of the Proposed Order filed concurrently herewith.

Respectfully submitted,

Date: August 26, 2011


 Ira M. Siegel, Cal. State Bar No. 78142
 email address: irasiegel@earthlink.net
 LAW OFFICES OF IRA M. SIEGEL
 433 N. Camden Drive, Suite 970
 Beverly Hills, California 90210-4426
 Tel: 310-435-7656
 Fax: 310-657-2187

Attorney for Plaintiff Digital Sin, Inc.

Exhibit 1

to

PLAINTIFF'S EX PARTE APPLICATION FOR LEAVE TO TAKE LIMITED DISCOVERY
PRIOR TO A RULE 26(f) CONFERENCE

UNITED STATES DISTRICT COURT

for the

District of NAME OF DISTRICT

Plaintiff's Name

Plaintiff

v.

Does 1-dddd

Defendant

Civil Action No. CV xx-xxxxxABC

(If the action is pending in another district, state where:
Northern District of California)SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

Custodian of Records, Comcast Cable Communications, 650 Centerton Road, Moorestown, NJ 08057

To:

☒ **Production:** **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and permit their inspection, copying, testing, or sampling of the material: Documents sufficient to identify the names, addresses, telephone numbers, and e-mail addresses of [ISP's] subscribers assigned the IP addresses identified on Attachment A on the corresponding dates at the corresponding times. You are to comply with this subpoena pursuant to the terms set forth in the Order attached hereto as Attachment B.

Place: LAW OFFICES OF IRA M. SIEGEL
433 N. Camden Drive, Suite 970
Beverly Hills, California 90210-4426

Date and Time:

[Set Out 70 Days from Service] *

☐ **Inspection of Premises:** **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:

Date and Time:

The provisions of Fed. R. Civ. P. 45(c), relating to your protection as a person subject to a subpoena, and Rule 45 (d) and (e), relating to your duty to respond to this subpoena and the potential consequences of not doing so, are attached.

Date: _____

*Compliance with this subpoena may be a multi-step process pursuant to the Order attached (Attachment B). At least the first step should be completed by [date 30 days out from service], with all steps completed by the date set forth under "Date and Time" above: [70 days out from service] (See paragraphs 4 and 5 of the Order.)

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

Attorney's signature

The name, address, e-mail, and telephone number of the attorney representing (name of party)

Plaintiff's Name

, who issues or requests this subpoena, are:

Ira M. Siegel, LAW OFFICES OF IRA M. SIEGEL, 433 N. Camden Drive, Suite 970, Beverly Hills, California 90210

email: irasiegel@earthlink.net

Tel: 310-435-7656

ATTACHMENT A

Table of Last-Observed Infringements by Defendants of Copyrights in Listed Motion Pictures that Are the Subject of Named Plaintiff's Listed Copyright Registrations

Defendant	Internet Protocol Address (IP)	Internet Service Provider (ISP)	Motion Picture Title/ Copyright Registration No.	Timestamp (North American Eastern Time)	Software
Doe xx	zz.zz.zz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xx	zz.zzz.zzz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xx	zz.zzz.z.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xx	zz.zz.zzz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zz.zz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xxx	zz.zz.zzz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zz.zzz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zz.zzz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xxx	zz.zz.zz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xxx	zz.zz.zzz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zzz.zzz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zzz.zz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zz.zzz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xxx	zz.zzz.zzz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent
Doe xxx	zz.zzz.zz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.z.zzz.zzz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss AM	BitTorrent
Doe xxx	zz.zz.zz.zz	ISP Name	Title of Work PA C-CCC-CCC	mm/dd/yyyy hh:mm:ss PM	BitTorrent

ATTACHMENT B

Ira M. Siegel, Cal. State Bar No. 78142
email address: irasiegel@earthlink.net
LAW OFFICES OF IRA M. SIEGEL
433 N. Camden Drive, Suite 970
Beverly Hills, California 90210-4426
Tel: 310-435-7656
Fax: 310-657-2187

Attorney for Plaintiff's Name

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

Plaintiff's Name, a California corporation,
Plaintiff,
v.
DOES 1-dddd,
Defendants.

CASE NO. CV xx-xxxxxx ABC

**ORDER GRANTING PLAINTIFF
LEAVE TO TAKE EARLY
DISCOVERY**

The Court, having reviewed Plaintiff's Ex Parte Application for Leave to Take Limited Discovery Prior to a Rule 26 Conference and the supporting documents submitted therewith, and good cause appearing therefore, hereby grants Plaintiff's Ex Parte Application and orders as follows:

[Balance of order as set forth by the Court]

Civil Action No. 10-04472 BZ

PROOF OF SERVICE*(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)*

This subpoena for *(name of individual and title, if any)* _____
 was received by me on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
 tendered to the witness fees for one day's attendance, and the mileage allowed by law, in the amount of
 \$ _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ 0 _____.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

Federal Rule of Civil Procedure 45 (c), (d), and (e) (Effective 12/1/07)**(c) Protecting a Person Subject to a Subpoena.**

(1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The issuing court must enforce this duty and impose an appropriate sanction — which may include lost earnings and reasonable attorney's fees — on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) Appearance Not Required. A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) Objections. A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing or sampling any or all of the materials or to inspecting the premises — or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the issuing court for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

(A) When Required. On timely motion, the issuing court must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person who is neither a party nor a party's officer to travel more than 100 miles from where that person resides, is employed, or regularly transacts business in person — except that, subject to Rule 45(c)(3)(B)(iii), the person may be commanded to attend a trial by traveling from any such place within the state where the trial is held;

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) When Permitted. To protect a person subject to or affected by a subpoena, the issuing court may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information;

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party; or

(iii) a person who is neither a party nor a party's officer to incur substantial expense to travel more than 100 miles to attend trial.

(C) Specifying Conditions as an Alternative. In the circumstances described in Rule 45(c)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(d) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:

(A) Documents. A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) Form for Producing Electronically Stored Information Not Specified. If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) Electronically Stored Information Produced in Only One Form. The person responding need not produce the same electronically stored information in more than one form.

(D) Inaccessible Electronically Stored Information. The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) Information Withheld. A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) Information Produced. If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(e) Contempt. The issuing court may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena. A nonparty's failure to obey must be excused if the subpoena purports to require the nonparty to attend or produce at a place outside the limits of Rule 45(c)(3)(A)(ii).

Exhibit 5

to

PLAINTIFF'S EX PARTE APPLICATION FOR LEAVE TO TAKE LIMITED DISCOVERY
PRIOR TO A RULE 26(f) CONFERENCE

BOXOFFICE.COM

New MPAA Chief Senator Chris Dodd Delivers Inaugural State of the Industry Speech

Add Comment on **March 29, 2011**

LAS VEGAS -- In his inaugural speech as CEO and Chairman of the Motion Picture Association of America, Inc. (MPAA), Senator Chris Dodd addressed exhibitors and spoke about the strong ties that bind motion picture studios and theater owners and their shared commitment to one of America's greatest industries. The following is the prepared text of Senator Dodd's keynote address at the National Association of Theatre Owners' CinemaCon:

Thank you, John, for that introduction and for NATO's continuing strong partnership. I'd also like to take a moment to thank Bob Pisano, who served as interim CEO this past year and represented the MPAA so well.

Today marks my ninth day on the job as Chairman and CEO of the Motion Picture Association of America. Despite the brevity of my tenure, I wanted to be here today to share with all of you my thoughts on the direction of our industry, and to listen to your concerns at what is both an exciting and challenging time for all of us.

Much of what I will say this morning I know you know, but at a moment like this, it is important that you know what I feel about this industry and the determination I bring to this undertaking.

So let me begin with the obvious: The production and exhibition industries cannot succeed - cannot survive - without each other. If you fail, we fail. And it's just as true that if we fail so will you.

We've come a long way together in the century since the first screening of a feature length motion picture in Jacob Stern's horse barn in Hollywood, California on February 14, 1914. Cecil B. DeMille invited 45 people (all of whom had worked on the film) to view "The Squaw Man," which he made for \$15,000. This premiere, if you want to call it that, was a total disaster.

In order to save some money, Mr. DeMille had purchased second-hand British equipment with ill-fitting sprockets, causing a technical malfunction that allowed the audience to only see the characters' hats, foreheads, boots and feet, and not much else. The economics of our industry have changed, of course, since that day in 1914. And, fortunately, so, too has the technology.

Last year the number of digital and 3D screens more than doubled - and our audience couldn't get enough of it. One in five dollars spent at the box office now comes from 3D. I can't help but wonder what Cecile B. DeMille, Sam Goldwyn, Louis B. Mayer, Jesse Lasky and Adolph Zucker and the rest of these pioneers would say if they could have been among the millions of moviegoers who marvel at the experience of seeing Avatar in a 3D theater. And like moviegoers here at home and all over the world, I can't wait, nor can you, I expect, to see what we come up with next.

But even though so much about our industry has changed over the years, the importance of the theater setting hasn't. Our films are still made to be shown on big screens in dark theaters filled with people. And no matter how our industry continues to evolve, I want all of you gathered here this morning to know that as the new CEO and Chairman of the MPAA, I passionately believe there remains no better way to see a movie than in a theater, and no more important relationship for our studios to maintain than the one we have with you.

So, when we saw box office growth in 2009, we cheered. In 2010 it slowed, and revenues dropped off in the early part of this year. That's not just a concern for you; it's a concern for all of us. But I for one do not believe the sky is falling. Yes, people have a wider variety of entertainment options these days. Yes, gas prices have gone up. But you have seen attendance ebb and flow in the past, and I believe audiences will be coming back to your theaters to see our films because there really is no parallel to the incredible experience that we, together, provide.

You are doing your part by building theaters with great seats, screens and sound systems. This week you'll be seeing some of the exciting projects our studios are working on to fill those seats and screens and sound systems with incredible entertainment later this year.

Thus, on my ninth day on the job, I've come here to commit myself to renewing and strengthening the great American movie-going tradition - and to ask you for your continuing partnership in tackling the challenges we must confront together.

It is, of course, undeniable that we do a fantastic job of providing the American people and others all over the world with quality entertainment. But, in my view, it is just as true that we must do a much better job of educating our audiences and the American people about how we do our job.

Let's begin with perhaps the single biggest threat we face as an industry: movie theft. At the outset, I want you to know that I recognize and appreciate that NATO members are on the front lines every day when it comes to

preventing camcording. Further, I want you to know that the member studios of the MPAA deeply appreciate the efforts you make every day to stop the hemorrhaging of movie theft in your theaters.



I am deeply concerned that too many people see movie theft as a victimless crime. After all, how much economic damage could there be to some rich studio executive or Hollywood star if a movie is stolen or someone watches a film that was stolen? It is critical that we aggressively educate people to understand that movie theft is not just a Hollywood problem. It is an American problem.

Nearly 2.5 million people work in our film industry. The success of the movie and TV business doesn't just benefit the names on theater marquees. It also affects all the names in the closing credits and so many more - middle class folks, working hard behind the scenes to provide for their families, saving for college and retirement. And since movies and TV shows are now being made in all 50 states, Puerto Rico and the District of Columbia, movie theft harms middle class families and small businesses all across the country.

Those who steal movies and TV shows, or who knowingly support those who do, don't see the faces of the camera assistant, seamstresses, electricians, construction workers, drivers, and small business owners and their employees who are among the thousands essential to movie making. They don't see the teenager working their first job taking tickets at the local theater, or the video rental store employees working hard to support their families.

We must continue to work together, pushing for stronger laws to protect intellectual property and more meaningful enforcement of those laws. We must also educate parents and students and everyone else about the real world impact of movie theft on jobs and on local tax revenues, and on our ability to make the kinds of movies and TV shows people wish to see.

At a time when too many Americans are out of work, we remain a major private sector employers, with more than \$140 billion in total wages spread out across a nationwide network of businesses. At a time when our trade deficit continues to spiral out of control, we are, to my knowledge, the only large American industry that maintains a positive balance of trade with every country in the world where we do business.

And speaking of trade, it goes without saying that we are all living and working in a global economy. It is therefore crucial to the survival and growth of the film business that we expand our reach around the world. The economics of our industry depends on the success of our films in all markets, not just our own. This issue is important to every single person in this room. To make the kind of great movies that fill seats in your theaters we must fill theaters in Russia, China, Brazil as well as other markets across the globe.

A larger audience overseas means more resources available for producing films here in America. And that, of course, means more films for distribution and exhibition, more seats filled, more popcorn sold. The good news about our industry is that whenever we're given the chance to compete in the world, we succeed. The bad news is we're not always given that chance to compete.

When China limits the import of non-Chinese films to 20 a year, despite the fact that hundreds of U.S. films are produced each year - including more than 100 by the MPAA member studios - we are excluded from a market that presents huge untapped potential.

I am confident that we can work together to ask Congress and others to protect intellectual property by cracking down on rogue websites that profit from the illegal trafficking of counterfeit movies. After all, you are not just our eyes and ears when it comes to illegal camcording - you are the face of the film industry in your local communities. No one is in a better position to educate the American public about these threats than are you.

After three decades in Congress, I have some idea how to attract the attention of a Congressman or Senator. When you return to your states, invite your local governor, state legislator, congressman and senator to your theater and fill it with those who work with you along with video store employees and their families. Tell them about the importance of these issues to you and to your communities. If you become that educator, you will leave a lasting and indelible impression on those who will make decisions about your future.

That's important not just because we sell a great product, but because all of us - studios, filmmakers and theaters alike - are preserving a great tradition, one that is as central to the American character, as it is important to the American economy.

Which brings me to my last point this morning. What I'm about to say isn't quantifiable in economic terms. I can't put a dollar figure on it for you. I can't give you an unemployment number or some other gripping statistic - but as I stand before you this morning one week into this job, I want you to know that it is as important as all data you will have thrown at you during CinemaCon. Our lives are getting more and more complicated. We are increasingly connected to the world by the power of emerging technologies, but at the same time we seem to be increasingly disconnected from each other by the same technology and stream of information and distractions.

And yet, in the midst of all of this, if you drop by a movie theater in America or anywhere around the world on a Friday or Saturday night you will see neighborhoods coming together. You will see people turning off their phones and BlackBerrys. You will see families and friends settling in for two hours in a darkened theater.

And even though everyone's eyes are on the screen, it is somehow still a communal experience - unlike any other. The value of that shared experience crosses economic, political and even generational boundaries.

Going to the movies together as a community has stitched together the fabric of American society in a way that few other institutions ever have or could, providing a nation of incredible diversity with a common cultural vocabulary and a common understanding of ourselves. What's at stake as we face these challenges is nothing short of the preservation and renewal of this quintessentially American communal tradition. Those who have come before us built the partnership between producers, distributors and exhibitors, which has sustained that tradition for almost a century.

It is my hope, and my commitment to you this morning that when those who follow us look back on this moment in our shared history, they will see that we did not walk away from the challenges we faced. Let them see that we stood together, attacking our challenges with the creativity and courage that have defined the larger-than-life story of American film from its humble beginnings at Stern's stable a century ago.

Like all good stories, this one features occasional moments of high drama. But for me, especially, this is just the first act. And I'm as excited by this new chapter in my life as I was when I first set foot in my local theater on a Saturday morning decades ago.

I'm so pleased that the first performance of this new chapter in my life has been with you. So pleased that the first person to introduce me to an audience, John Fithian, is someone who I've known for half my life and almost all of his.

I'm proud to be a small part of this great American business, and most importantly, I'm honored to be in your company. Your theaters have given America and the world hours of joy and lifetimes of memories. I look forward to working with you closely in the days ahead.

© 2011 BOXOFFICE Media, LLC. All rights reserved.

support@boxoffice.com

Exhibit 6

to

PLAINTIFF'S EX PARTE APPLICATION FOR LEAVE TO TAKE LIMITED DISCOVERY
PRIOR TO A RULE 26(f) CONFERENCE



Log In ! Online Subscription Help Language Dictionary

Search variety.com

SEARCH

Home | 4/13/2011 10:11 A.M. | Text size: a⁻ a⁺

Subscribe to VARIETY at 73% off the cover price

Latest News	Latest Reviews	Features	People News	Charts	Opinions	Events	Photos	Videos	VarietyMediaCareers.com
FILM	TV	LEGIT	MUSIC	TECH	INTERNATIONAL				Archives

Technology News

Posted: Wed., Apr. 13, 2011, 4:00am PT

Share Print

Joe Biden talks piracy strategy with Variety

VP's involvement with issue extends back two decades

By TED JOHNSON

Exclusive: When Vice President Joseph Biden appeared at a news conference last summer about copyright theft, he compared it to "smashing the window at Tiffany's and reaching in and grabbing what's in" the store.

It was just the kind of hard-line rhetoric that studios and record labels have been yearning to hear from Washington, but even more significant was that it was coming from the nation's No. 2.

One of Biden's friends, former Sen. Christopher Dodd, the new chairman of the Motion Picture Assn. of America, said that Biden isn't just reading from a script when it comes to content protection.

"Joe believes it passionately and understands it intellectually. The marriage of those two doesn't always happen in this town."

If anything, the administration's anti-piracy efforts have been extensive enough to generate criticism from some consumer and digital rights groups that they are too heavy handed. A federal crackdown, which shutdown more than 120 sites trafficking in pirated content, already raised concerns that legitimate sites are being swept up in the effort. And although the issue tends to cross partisan lines, Biden and the administration have strong ties to Hollywood, which was a huge source of donor support for Barack Obama's campaign, and is expected to play a significant role in his reelection campaign.

The White House, however, was mandated to take a greater role in addressing piracy: A law passed in 2008 and signed by President George W. Bush required the establishment of an intellectual property enforcement coordinator, or a so-called "IP czar." Drawing more attention to the issue, Biden has appeared several times with IP coordinator Victoria Espinel, including when she has unveiled a strategic plan in June.

In written responses to a series of questions submitted by Variety, Biden said his involvement with the piracy issue extends back two decades to when he was chairman of the Judiciary Committee, and that his use of the bully pulpit "is really just a continuation of that work."

"Look, piracy is outright theft," Biden said. "People are out there blatantly stealing from Americans -- stealing their ideas and robbing us of America's creative energies. There's no reason why we should treat intellectual property any different than tangible property."



Vice President Joseph Biden told Variety that showbiz needs to do a better job of marketing its anti-piracy pitch.

Email or Share Print
RSS Feed Bookmark

Get Variety:

Mobile Digital Newsletters

Subscribe to Variety

-- Advertisement --

We've got great things in "score" for you!

ASSETS: WORLD-CLASS MUSICIANS, WORLD-CLASS SCORES
LIABILITIES: N/A

CALL US: 818.755.7777

PROUD MEMBER: HollywoodGreenTeam.org

FILM MUSICIANS SECONDARY MARKETS FUND
www.fmsmf.org

-- Advertisement --

He is quick to say that he considers it more than a problem of just the entertainment industry. "When our military is sold counterfeit equipment that is faulty, it affects our national security. And when cancer patients are sold fake cancer drugs that contain no medicine, it affects public health. These are serious issues for the American people."

"Virtually every American company that manufactures something is getting killed by counterfeiters: clothing, software, jewelry, tires," Biden said. "If an American company has been successful at developing an idea, it's likely getting stolen."

But getting that point across has been difficult.

Although the MPAA and studios have for years run PSA campaigns, they have been of questionable effectiveness.

And while Biden tries to connect the issue to the average worker, in the minds of middle America Hollywood is red carpets, lavish salaries and Charlie Sheen.

"I think the entertainment industry would agree that they have done a poor job in making their case and need to do better," Biden said. "I mean, they have some of the brightest and most creative people working for them."

"They should be able to come up with an intelligent, original and effective public education campaign targeting this issue. To be honest, I am not certain they have dedicated the appropriate resources to this, and I hope they will."

He says that the administration also sees a government role in a public awareness campaign, which is "a big part of our strategy." The Justice Department is providing funds to the National Crime Prevention Council, including messages geared toward kids.

"Kids are taught that it is not right to steal a lollipop from the corner store," he said. "They also need to understand that it is equally wrong to knowingly steal a movie or a song from the Internet."

Biden held an "intellectual property summit" in December, 2009 that brought together cabinet secretaries as well as studio chiefs and reps from other copyright industries, with the intent of mobilizing enforcement efforts. Fox Filmed Entertainment co-chairman and CEO Tom Rothman, who attended another gathering in January that included Attorney General Eric Holder and Secretary of Commerce Gary Locke, said that "in many ways [Biden's] personal commitment to it is a breakthrough for us" as he has tied "the issue's importance to the overall health of the American economy."

Biden doesn't buy the idea that Hollywood's effort to increase enforcement is merely to protect dying businesses.

"The fact is, media companies have already taken significant steps to adapt their business models to keep up with changes in how we watch movies and listen to music," Biden said. "Content is being offered to consumers in a variety of different ways that make it easy and cost-effective for people to access legal material. Anyone who does not understand this should simply talk with one of my grandkids."

In the next few weeks, legislation is expected to be introduced to give federal prosecutors and customs officials a quicker process to get sites offering pirated content shut down, as well as to choke the money supply flowing to foreign sites from payment processors and ad firms.

A version of the bill passed the Senate Judiciary Committee unanimously late last year, but Sen. Ron Wyden (D-Oregon) helped block it from going to the floor because of concerns that it could infringe on free-speech rights. Biden said he's been working with senators to craft legislation "that helps protect property while at the same time respects any potential Constitutional issues. I am hopeful that we will be able to reach an agreement that is agreeable to all parties."

Where Biden says he hopes "we won't need to legislate" is in industry efforts to get Internet providers to inform their customers when they have downloaded or streamed pirated content. Under a "three strikes" law in France, customers who repeatedly view infringing content risk having their service suspended.

Instead, Biden's office has been working with studios and record labels and Internet providers to reach some kind of voluntary agreement to establish standards "that provides greater education to those who might be downloading or streaming illegal content."



Britweek Film and TV Summit
April 29, 2011
Beverly Hilton Hotel, Los Angeles, CA

Entertainment & Technology Summit
May 2, 2011
The Ritz-Carlton, Marina Del Rey, CA

2nd Annual International Film Finance Forum
May 13, 2011
Hotel Majestic Barriere, Cannes, France

Film Finance Forum @ Screen Singapore
June 7, 2011
Capella Resort, Sentosa Island, Singapore

3D Entertainment Summit™
June 21-22, 2011
Hilton New York, New York, NY

NY Mobile Entertainment Summit™
June 21-22, 2011
Hilton New York, New York, NY

[View all Conferences and Events](#)



Variety Luxury
REAL ESTATE
[CLICK HERE FOR LISTINGS](#)

Biden said he sees a shift in China, where piracy is rampant and where Hollywood has long struggled to gain cooperation from the government to address the problem. He said South Korea's strengthened intellectual property laws have led to the "Korean Wave" in entertainment across Asia, and "China's leaders understand this."

When President Hu Jintao visited the U.S. in January, China agreed to take new steps to protect copyrighted material, but Biden said that further efforts will be required "if China is to fulfill its ambition to build a more innovative economy."

Biden is being presented with one of the Recording Academy's Grammys on the Hill awards today.

Contact Ted Johnson at ted.johnson@variety.com

GUEST, HERE ARE OTHER ARTICLES RECOMMENDED FOR YOU...

[Joaquin Phoenix in talks to join Anderson pic](#)

['Pirates of the Caribbean' plans trip to Cannes](#)

[Joe Biden talks piracy strategy with Variety](#)

Powered by  newstogram

Read Next Article: [Chromatic chaos reigns >](#)

© Copyright 2011 **RBL**, a division of Reed Elsevier Inc.

[Subscribe](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [About Us](#) | [Advertise](#) | [Contact Us](#) | [Sitemap](#) | [Help](#)

Media: [LA 411](#) | [New York 411](#) | [Variety](#)

Construction: [Reed Construction Data](#)

Business Directory: [HotFrog](#)

Exhibit 8

to

PLAINTIFF'S EX PARTE APPLICATION FOR LEAVE TO TAKE LIMITED DISCOVERY
PRIOR TO A RULE 26(f) CONFERENCE



Technical report:
An Estimate of Infringing Use of the Internet

January 2011

Version 1.8
Envisional Ltd,
Betjeman House,
104 Hills Road,
Cambridge,
CB2 1LQ

Telephone: +44 1223 372 400
www.envisional.com
piracy.intelligence@envisional.com



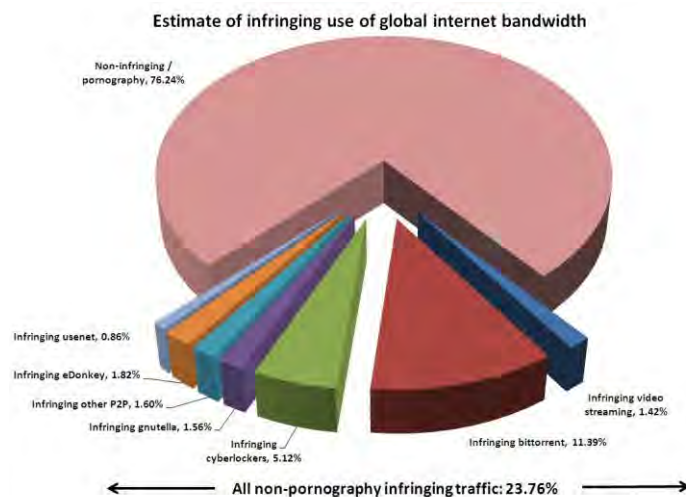
1 Introduction

Envisional was commissioned by NBC Universal to analyse bandwidth usage across the internet with the specific aim of assessing how much of that usage infringed upon copyright. This report provides the results of that analysis and is in three main parts.

- **Part A** examines the internet arenas most often used for online piracy – peer-to-peer networks (with a specific focus on bittorrent), cyberlockers (file hosting sites such as Rapidshare), and other web-based piracy venues (such as streaming video) – and estimates the proportion of infringing content found on each.
- **Part B** is a critical analysis of recent studies from four network equipment and monitoring companies. These companies measured network traffic at multiple (and different) sites worldwide to characterize overall internet usage.
- **Part C** combines the data and analysis from Part A and Part B in an attempt to show what proportion of internet traffic represents unauthorised distribution of copyrighted material.

1.1 Executive Summary

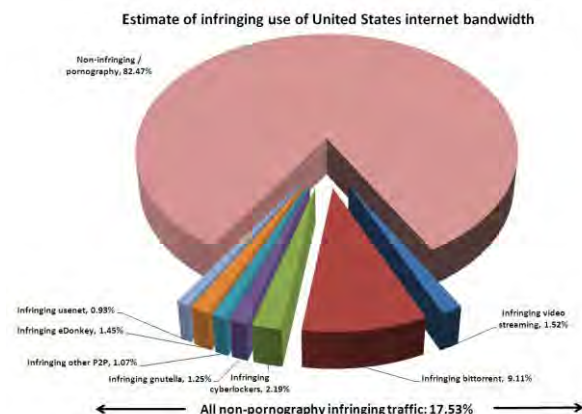
- Across all areas of the global internet, **23.76% of traffic was estimated to be infringing**. This excludes all pornography, the infringing status of which can be difficult to discern.
- The level of infringing traffic varied between internet venues and was highest in those areas of the internet commonly used for the distribution of pirated material.



- **BitTorrent traffic** is estimated to account for 17.9% of all internet traffic. Nearly two-thirds of this traffic is estimated to be non-pornographic copyrighted content shared illegitimately such as films, television episodes, music, and computer games and software (63.7% of all bittorrent traffic or 11.4% of all internet traffic).
- **Cyberlocker traffic** – downloads from sites such as MegaUpload, Rapidshare, or HotFile – is estimated to be 7% of all internet traffic. 73.2% of non-pornographic cyberlocker site traffic is copyrighted content being downloaded illegitimately (5.1% of all internet traffic).

- **Video streaming traffic** is the fastest growing area of the internet and is currently believed to account for more than one quarter of all internet traffic. Analysis estimates that while the vast majority of video streaming is legitimate, 5.3% is copyrighted content and streamed illegitimately¹, 1.4% of all internet traffic.
- Other **peer to peer networks and file sharing arenas** were also estimated to contain a significant proportion of infringing content. An examination of eDonkey, Gnutella, Usenet and other similar venues for content distribution found that on average, 86.4% of content was infringing and non-pornographic, making up 5.8% of all internet traffic.
- In the **United States**, 17.53% of Internet traffic was estimated to be infringing. This excludes all pornography. A breakdown of internet usage yields the following results:

- Peer to peer networks were **20.0% of all internet traffic** with bittorrent responsible for 14.3%. The transfer of infringing content located on these networks comprised 13.8% of all internet traffic.
- **Video streaming made up between 27% and 30% of traffic**, though only a small percentage of this was believed to be infringing (1.52%)
- **Cyberlocker traffic was estimated at 3%** of all network traffic and infringing use was estimated at 2.2% of all internet traffic.



Given the enormous, ever-growing, and constantly-changing size, shape, and consistency of the internet and the use that is made of it means that methodological issues abound when attempting to produce measurements of traffic and content. Yet even given the limitations of the data available, Envisional believes that the estimates produced in this report are more accurate than any that have been published before. This report draws together the data in a way that allows, for the first time, the organisations which can help shape the ways in which users interact and obtain content to understand how much of the internet is devoted to the distribution and consumption of infringing material.

Piracy Intelligence

Envisional Ltd



¹ Mostly from hosts commonly used for pirated content such as MegaVideo and Novamov rather than sites more often used for legitimate user generated content such as YouTube and DailyMotion, for instance.

2 Part A: Internet Usage Assessment

2.1 Introduction

Part A of this report examines the major arenas of the internet known to be used – either primarily or as one of a number of uses – to distribute pirated content. Included in our analysis are:

- BitTorrent
- Cyberlockers
- Video streaming sites
- eDonkey and Gnutella
- Usenet

For each, we estimate the percentage of available content likely to be infringing. Then, in Part C, we translate these individual percentages into estimates of Internet traffic – to do this we rely upon data from studies into network traffic that were conducted by a range of vendors last year and which are discussed in detail in Part B. These individual estimates of infringing traffic are used to yield an estimate of the overall percentage of global internet traffic that results from their use (and which is infringing).

2.2 Executive Summary

Our major findings for each of the four major areas of our investigation follow.

BitTorrent

- BitTorrent is the most used file sharing protocol worldwide with over 8m simultaneous users and 100m regular users worldwide.
- Over 2.72m torrents managed by the largest bittorrent tracker were examined for this report. Our analysis suggests nearly two-thirds of all content shared on bittorrent is copyrighted and shared illegitimately.²
- An in-depth analysis of the most popular 10,000 pieces of content managed by PublicBT found:
 - **63.7% of content managed by PublicBT was non-pornographic content that was copyrighted and shared illegitimately**
 - 35.2% was **film** content – all of which was copyrighted and shared illegitimately

² PublicBT (publicbt.com) is the largest and most popular bittorrent “tracker” worldwide. A recent Envisional survey found that all of the most popular content listed on two popular portals referenced PublicBT trackers. With 2.72 million torrent files available in December 2010, PublicBT is believed to have comprehensive coverage of most files transferred using bittorrent and is therefore a suitable proxy for anyone seeking to assess the percentage of those transfers that infringe copyrights.

- 14.5% was **television** content – all of which was copyrighted and shared illegitimately. Of this, 1.5% of content was Japanese anime and 0.3% was sports content.
 - 6.7% was **PC or console games** - all of which was copyrighted and shared illegitimately
 - 2.9% was **music** content – all of which was copyrighted and shared illegitimately
 - 4.2% was **software** – all of which was copyrighted and shared illegitimately³
 - 0.2% was **book** (text or audio) or **comic** content – all of which was copyrighted and shared illegitimately
 - 35.8% was **pornography**, the largest single category. The copyright status of this was more difficult to discern but the majority is believed to be copyrighted and most likely shared illegitimately⁴
 - 0.48% (just 48 files out of 10,000) could not be identified
- Of all 10,000 files comprising the most popular content held on the PublicBT tracker, **only one was identified as non-copyrighted** (a file containing a list of IP addresses used to help users guard against spam and peer to peer monitoring). There is no evidence to support the idea that the transfer of non-copyrighted content such as Linux distributions makes up a significant amount of bittorrent traffic.⁵
 - Analysis strongly indicates that private bittorrent sites (which would not usually make use of PublicBT) are overwhelmingly used for the purposes of illegitimately sharing copyrighted data.

eDonkey and Gnutella

- Analysis of known copyrighted and non-copyrighted material on the eDonkey network suggests that the vast majority of content held and transferred on the network is likely copyrighted (98.8%).
- Similar analysis using search queries on Gnutella found that most users on the network appeared to be looking for copyrighted content: 94.2% of non-pornographic search queries which could be identified were apparently for copyrighted material.

Cyberlockers

- An examination of 2,000 random links pointing to content held on cyberlockers found that 91.5% of links pointing to non-pornographic material were linking to copyrighted material, or 73.15% of all links.

³ A very small proportion (0.13% of the top 10,000 or 13 individual files) was cracks aimed at removing the copy protection from copyrighted software such as Windows 7 or Microsoft Office.

⁴ For the purposes of this report, the copyright status of any pornography identified is ignored, though the piracy of such content is obviously of interest to the adult video industry (reflected in the many legal suits filed against downloaders during 2010).

⁵ Similar analysis conducted by Envisional in December 2009 found only a single Linux distribution as the only piece of non-copyrighted content in the top 10,000 torrents shared by OpenBitTorrent, then the largest bittorrent tracker online.

Video streaming sites

- A comparison of video streaming site usage estimated that 4.7% of video streaming data traffic is copyrighted content illegitimately streamed from video hosting sites.

Usenet

- Analysis of content posted to a number of Usenet newsgroups found that at least 93.4% of posts contained copyrighted material.

2.3 Discussion: BitTorrent

All available data strongly suggests that bittorrent is the most used file sharing protocol worldwide. Part B of this report contains data conservatively estimating that bittorrent usage makes up 14.6% of *all* internet bandwidth worldwide. Envisional consistently measure over eight million users simultaneously connected to the bittorrent network and the distributor of two of the most-used bittorrent clients, uTorrent and BitTorrent Mainline, claims that the clients have over 100 million unique users worldwide and 20 million daily users⁶.

This section of the report aims to establish what proportion of the data transferred through bittorrent is legitimate and approved by the content owner and what proportion is illegitimate and copyrighted. This is a complicated task. The estimate provided here is produced from a number of data points but primarily from a major investigation into the activities of the largest public bittorrent tracker, PublicBT.

2.3.1 Tracker Analysis

Much of the communication on bittorrent takes place with the aid of a central server called a *tracker*. A tracker helps users on bittorrent find those who are already downloading or uploading the file or files in which they are interested. The tracker records the IP addresses of those actively involved in obtaining or distributing a particular file and then shares them with other bittorrent users when requested.⁷

Trackers also record data on each **torrent or file** which they track: this data includes the 'hash' of that file (a unique code that identifies that file alone) as well as the number of **seeds** (users holding an entire copy of the file), **leechers** (users in the act of downloading), and (in most cases) total completed **downloads**. Trackers do not tend to record file names.

The largest tracker worldwide is the **PublicBT tracker**. At the point that this analysis was conducted, it held information on over 2.7m individual torrents⁸. Launched in 2009, the tracker



became the most-used tracker for bittorrent swarms during 2010. PublicBT is simple to use, open to any bittorrent user, and free. It has also proved very reliable during its life to date. PublicBT does not cover *every* file available on bittorrent: bittorrent users are free to create torrents using any trackers of their choice and some niche content – such as sport broadcasts or technical ebooks – may be more often found at private trackers which require

⁶ <http://www.businesswire.com/news/home/20110103005337/en/BitTorrent-Grows-100-Million-Active-Monthly-Users>

⁷ Trackers are not the only way to obtain IP addresses: bittorrent clients can also communicate through a decentralised network overlay. Additionally, some clients will swap IP addresses of known downloaders or uploaders of a specific file in a transaction known as 'peer exchange', though they must have already managed to locate the other client in the first place. However, trackers are used as the first port of call in almost all torrent downloads and are likely to be the source of a significant proportion of the IP addresses gathered by a client.

⁸ <http://publicbt.com/>

registration. However, analysis of the most popular 100 torrents on two popular portals (ThePirateBay, the most used portal worldwide and Torrentz⁹) found that every single torrent listed could be found on the PublicBT tracker, indicating that PublicBT can be assumed to have close to comprehensive coverage of the content that is most downloaded on bittorrent. The sheer size of the tracker also means that such coverage will be deep and broad.

Envisional was able to gather data on **every file tracked by PublicBT** on a specific day. This data was then used in an attempt to estimate the amount of legitimate against illegitimate and copyrighted content carried by the tracker. On the day of analysis (a weekday in mid-December 2010), PublicBT held information on **2.72m individual torrent swarms** and managed connections from just over **19.5m peers**.¹⁰

The analysis below examines the characteristics of all the 2.72m torrent swarms found on PublicBT. A detailed study was also made of the 10,000 torrents managed by PublicBT that had the most active downloaders, in order to better understand the make-up of the most sought-after content on bittorrent. An analysis of these swarms found that pornography, film, and television were the most popular content types. Further, with pornography excluded, **only one identified swarm in the top 10,000 offered legitimate content** (a file holding a list of IP addresses used to guard users against spam and peer to peer monitoring).

2.3.2 Summary analysis

On the day chosen for analysis of PublicBT, **2,721,440 torrents** were being managed by the tracker. These are unique files but the figure does not mean 2.72m different films or television episodes or pieces of music. There may be many different copies of a specific film title available through PublicBT – for instance, at different file sizes or in different formats or different qualities (as an example, seventy-one different versions of the film *Inception*, one of the most popular titles at the time of analysis, were located in the top 10,000 torrents).

Each file available on bittorrent is identified by a unique ‘hash’ – a unique code that identifies that file and no other.¹¹ PublicBT thus held information on the active downloaders and uploaders of just over 2.7m unique hashes.

⁹ www.thepiratebay.org and www.torrentz.me

¹⁰ This does not mean 19.5m individual users: a peer connected to two torrents will be counted twice in that total of peers due to the nature of bittorrent. It is not possible to know the average number of swarms to which an average user is connected at any one time. However, even assuming that each user is connected to nineteen torrents tracked by PublicBT (a very high estimate judging on anecdotal evidence) would still mean that 1m individual users were connected to PublicBT, around one-eighth of the total simultaneously connected bittorrent population of 8m. A more likely possibility is that most users connect to far fewer swarms and that PublicBT activity reflects a large proportion of public bittorrent transfers.

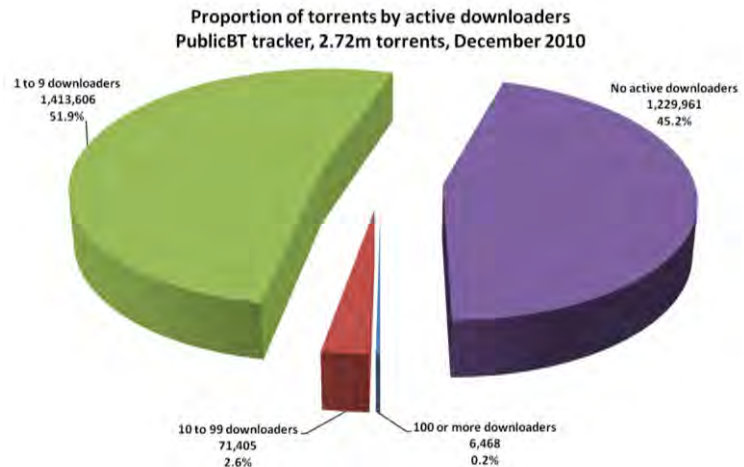
¹¹ A “hash” is a unique alpha-numeric sequence used to identify files (movies, music, documents, etc) on bittorrent. On the bittorrent network, the hash is generated by the SHA1 algorithm which creates a small identifier from a large file (such as a movie). Even trivial modifications to the original file results in a completely different hash.

Content analysis

On the day of analysis, most upload and download activity was concentrated amongst a **small number** of those 2.7m torrents with 34.9% of all peers involved in the top 10,000 (just 0.37% of all torrents). There was an **enormous long-tail of content** which had only a few or no seeds or a few or no leechers.

The chart shows the breakdown of all 2.72m swarms according to the number of downloaders (commonly called leechers) attached to each swarm¹². Clearly, most of the swarms had only a small number of active downloaders or no active downloaders at all.

- 0.2% of torrents (6,468) had 100 or more downloaders
- 2.6% of torrents (71,405) had from ten to 99 downloaders
- 51.9% of torrents (1,413,606) had from one to nine downloaders
- 45.2% of torrents (1,229,961) had no active downloads



A similar spread was evident for seeders (users holding a complete copy of the file). For almost **half of all torrents** (1.32m or 48.5%), no seed was connected.

On the other hand, a very small overall proportion of content attracted large numbers of downloaders, representing a large proportion of all connected users. As stated above, torrent swarms with 100 or more downloaders represented just 0.24% of the available 2.72m torrents, but more than one in three – 30.4% - of all peers connected to PublicBT. Torrents with ten or more downloaders represented 2.6% of the 2.72m available torrents but over half – 53.9% - of all peers.

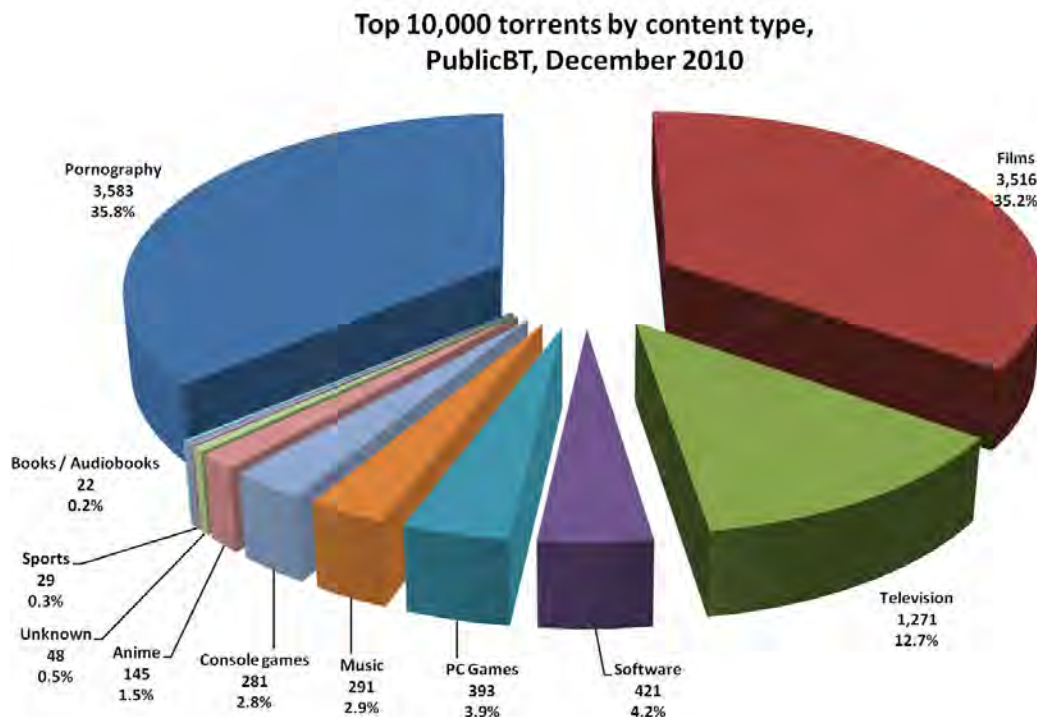
¹² This report uses the term 'swarm' even where no participants were actively sharing content (for instance, where there were no downloaders or no seeds). Technically perhaps, a torrent for which there is a tracker and a seed but no downloader should be known as a 'potential swarm' or similar but the term 'swarm' is retained for the sake of simplicity and understanding.

Analysis of the top 10,000 torrent swarms

To determine the percentage of infringing content associated with PublicBT, Envisional made a thorough analysis of **the top 10,000 swarms** (as determined by the number of downloaders). This is a small sample of the overall number of torrents (0.37%) but represents **34.9% of all peers** connected to PublicBT. To put it another way, more than one-third of all connections to PublicBT were interested in just 0.37% of the swarms managed by the tracker, showing a strong interest in a very small proportion of content. The seeds connected to these most popular 10,000 swarms were 35.5% of all seeds while the downloaders were 33.8% of all leechers.

The content being shared by each swarm in the top 10,000 was verified in almost every case using various methods¹³. Overall, **9,952 of the top 10,000 swarms were identified and confirmed** (99.52%) with only 48 swarms containing unknown content.¹⁴

The chart shows the distribution of swarms by content type with video dominating overall. Pornography video was the largest single type at 35.8% of all of the top 10,000 torrents. Film was the second largest type at 35.2%, followed by television episodes at 12.7%. Japanese anime episodes added a further 1.5% and sports broadcasts another 0.3%. These results mean that **85.5% of all of the top 10,000 torrents were video content of some kind**.

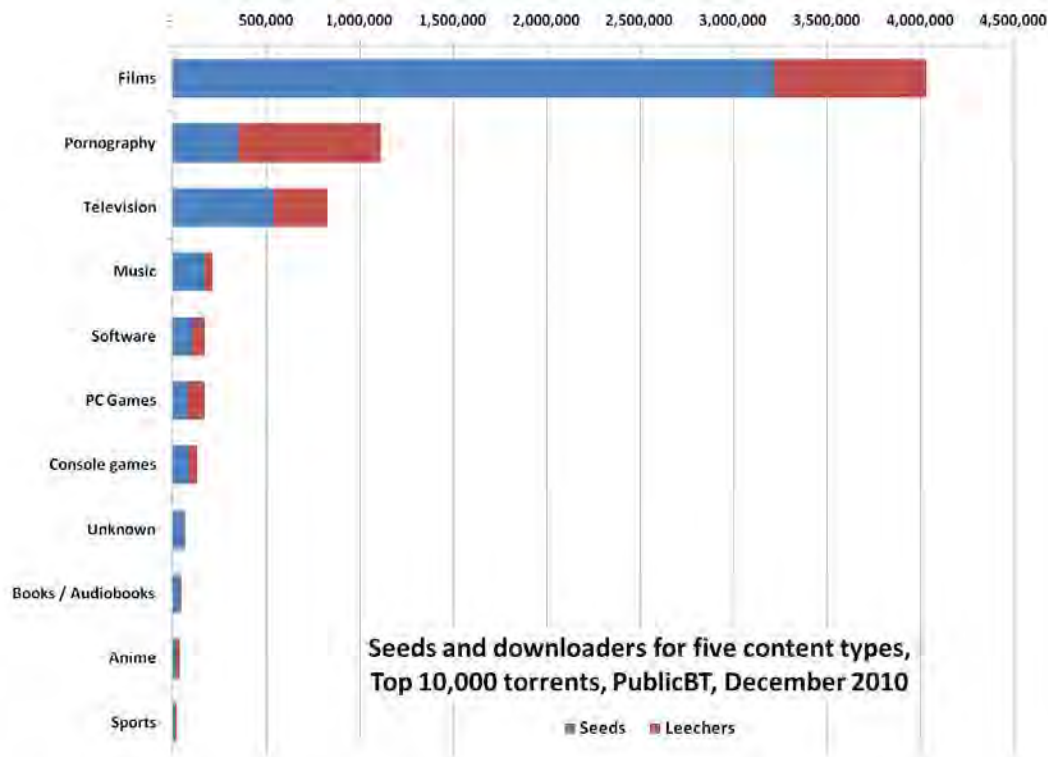


¹³ In most cases, the hashes for each torrent were checked against a range of torrent portals for verification. For many video files, a section of the file was downloaded and viewed.

¹⁴ Note that the analysis of the top 10,000 swarms contained here does not include 139 files which contained enough leechers to merit inclusion within the top 10,000 but were found to be fake. Fake files are often uploaded to bittorrent by interdiction companies hoping to confuse downloaders or by virus and malware distributors. The top 10,000 is therefore **the top 10,000 non-fake files** – or to put it another way, the top 10,139 files with the fake files removed.

Software comprised 4.2% of all of the top 10,000 torrents with computer games adding 6.7% (PC games were the largest proportion at 3.9% and console games contributed 2.8%). Music was 2.9% of the total with books (including comics) and audiobooks adding 0.2%. The remaining 0.5% of torrents could not be identified.¹⁵

The chart below looks at the number of seeds and downloaders for each content type within the top 10,000 torrents: again, video content – particularly film – gathered the largest number of seeds and downloaders (indicating strong demand and strong supply)¹⁶. In total, just over **4.0m peers were seeding or downloading a piece of film content** located in the top 10,000 torrent swarms on PublicBT at the point that this sample was taken. This is 59.2% of all peers connected to the top 10,000 swarms.



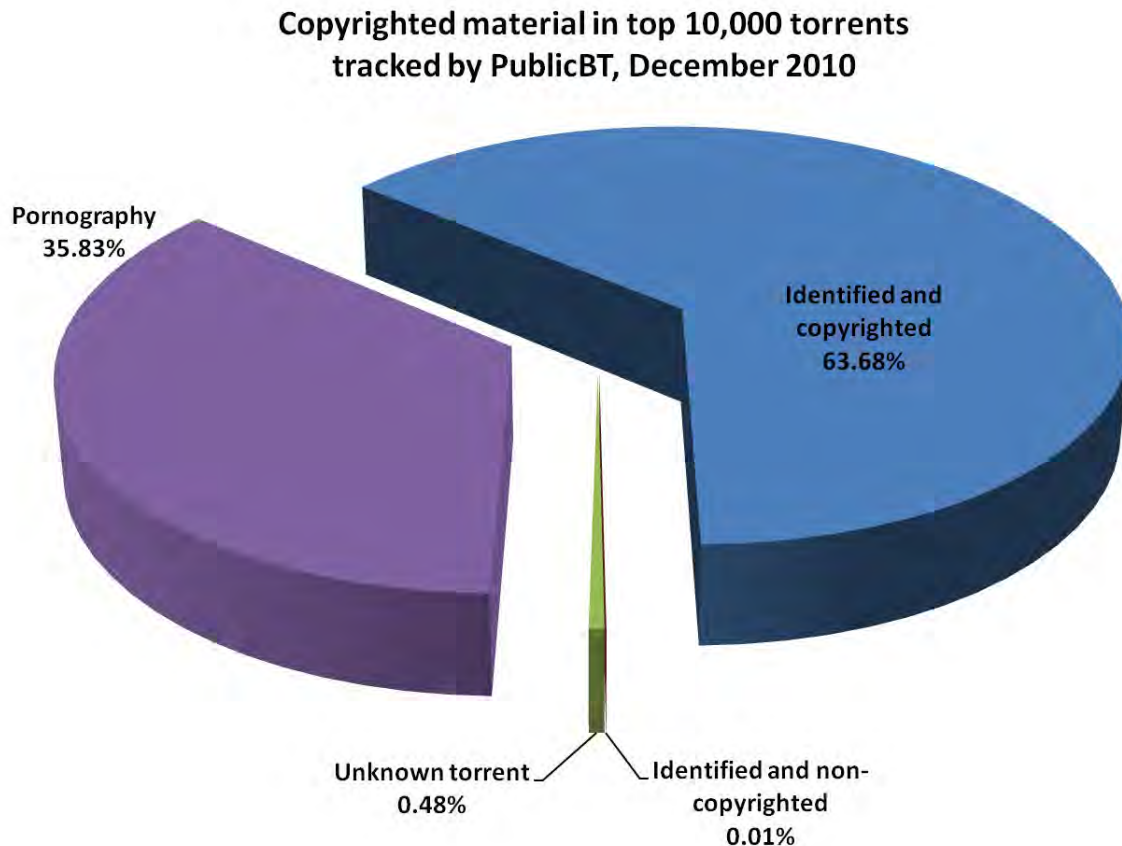
While pornography was the largest single type by numbers of torrents, there were many fewer total peers, principally because there were many fewer seeds than for film content. 828,000 peers were seeding or downloading television content and there were much lower numbers for the remaining content types in the top 10,000 torrents. Across all categories, peers connected to swarms for video content (films, television, anime, sports, and pornography) made up 88.4% of all peers in the swarms for the top 10,000 torrents.

¹⁵ Overall, this analysis is similar to that conducted by Envisional in December 2009 on the OpenBitTorrent tracker, though the current effort successfully identified significantly more torrents. The earlier analysis could not identify 25.0% of the top 10,000 torrents though most of these unidentified torrents were believed to be pornography. The more recent analysis reported here suggests that this belief was correct.

¹⁶ Numbers for seeders and downloaders were taken from PublicBT during the period of analysis.

Proportion of copyrighted material

As noted, the contents of 9,952 swarms were identified and verified. Excluding the swarms containing pornography (3,583 swarms or 35.83%) provides 6,369 pieces of verified content. Of these identified swarms, **only one was found to contain non-copyrighted content**. This was a torrent containing a list of IP addresses used to help peer to peer users block spam results and fake content.¹⁷



With the pornography content discarded, this means that at a minimum, **99.24% of the top 10,000 files managed by the PublicBT tracker** were copyrighted material with the rest of the content unknown (0.75%) or non-copyrighted (0.01%).

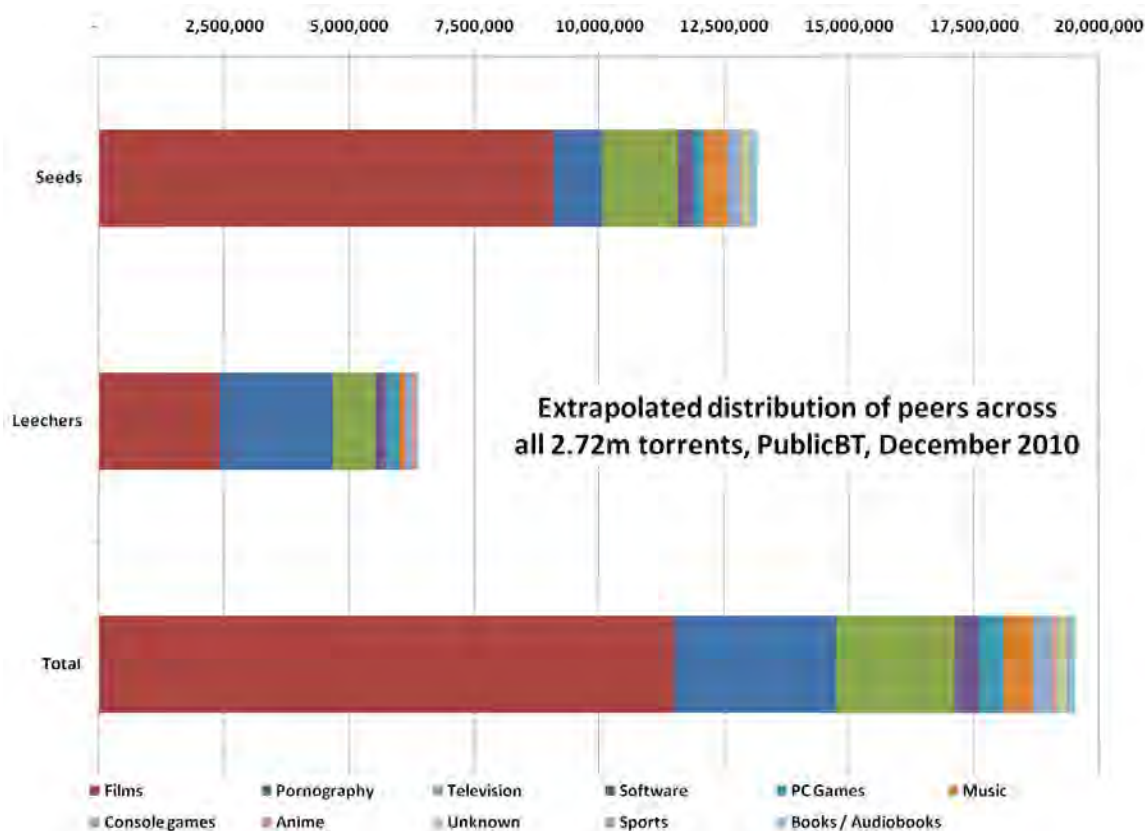
Analysis of content from outside the top 10,000 torrents found a similar dominance of copyrighted material. Five samples, each of 100 torrents, were taken from various points in the long tail of PublicBT content. Discarding

¹⁷ The file was named "hostiles.txt". The torrent hash was a55603e3b98fb51fd05fb2ed3fbc2b2c6d254c6e. The results mirror the Illinois State University study conducted by Jon Peha and Alex Mateus (Carnegie Mellon University) in which it is noted: "...there is no evidence to support the hypothesis that the transfer of Linux distributions is a driver for the use of P2P, even among users that do not use P2P for copyrighted material." See *Dimensions of P2P and digital piracy in a university campus*: http://www.ece.cmu.edu/~peha/dimensions_of_piracy.pdf

pornography, no non-copyrighted content was located in these samples though there was a slightly higher spread of unknown material (as might be expected from less popular content).¹⁸

Extending the results

If the figures underlying the chart above for the top 10,000 torrents are extrapolated to all of the content present on PublicBT, it would mean that on the day of analysis, **11.5m peers were seeding or downloading film content** through the PublicBT tracker, **2.4m peers were seeding or downloading television content**, 3.2m pornography, 593,000 seeding or downloading music, and 862,000 games.¹⁹ The chart shows the result of this calculation and the table over provides further details.



¹⁸ This result accords with past analysis which have indicated that the majority of content offered on torrent portals is infringing. For instance, Judge Steven Wilson noted in his Isohunt decision that “In a study of the Isohunt website, [Dr. Richard] Waterman [of the University of Pennsylvania] found that approximately 90% of files available and 94% of dot-torrent files downloaded from the site are copyrighted or highly likely copyrighted.”

http://www.wired.com/images_blogs/threatlevel/2009/12/fungruling.pdf

¹⁹ For instance, 69.05% of all seeds for the top 10,000 swarms were involved in swarms for film content (3,220,293 seeds). Assuming that 69.05% of seeds across all swarms were involved in swarms for film content provides an extrapolated figure of 9,084,608 seeds.

Envisional: Internet bandwidth usage estimation

14

	Seeds			Downloaders (leechers)			Total
Content type	Seeds in top 10,000 swarms	Percent of all seeds in top 10,000	Estimated seeds across all swarms	Downloaders in top 10,000 swarms	Percent of all downloaders in top 10,000	Estimated downloaders across all swarms	Total peers (seeds plus downloaders)
Films	3,220,293	69.05%	9,084,608	812,648	37.73%	2,404,271	11,488,879
Pornography	347,618	7.45%	980,648	766,157	35.57%	2,266,725	3,247,372
Television	538,607	11.55%	1,519,437	289,426	13.44%	856,285	2,375,723
Music	170,989	3.67%	482,369	37,399	1.74%	110,647	593,016
Software	99,645	2.14%	281,104	71,259	3.31%	210,824	491,928
PC Games	78,543	1.68%	221,574	91,059	4.23%	269,404	490,978
Console games	85,118	1.83%	240,122	44,148	2.05%	130,615	370,737
Unknown	58,687	1.26%	165,559	6,630	0.31%	19,615	185,174
Books (incl. audiobooks)	41,621	0.89%	117,415	2,777	0.13%	8,216	125,631
Anime	12,536	0.27%	35,365	24,211	1.12%	71,630	106,994
Sports	10,337	0.22%	29,161	8,046	0.37%	23,805	52,966

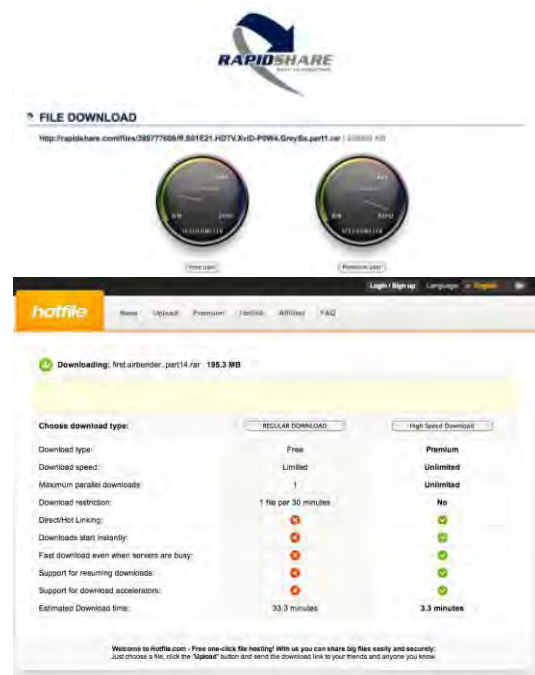
2.4 Discussion: Cyberlockers / File hosting sites

Over the last two years, various technological factors such as the decline in the cost of data storage combined with the increasing use of the web as the most important and central part of the internet for most users have led to the appearance and increasing use of what have become widely known as 'cyberlockers': centralised file storage services to which individuals can upload material for access by themselves or others. There are a number of widely used cyberlockers such as **MegaUpload**, **4Shared**, **Rapidshare**, and **Hotfile**. Envisional monitor over one hundred different cyberlockers.

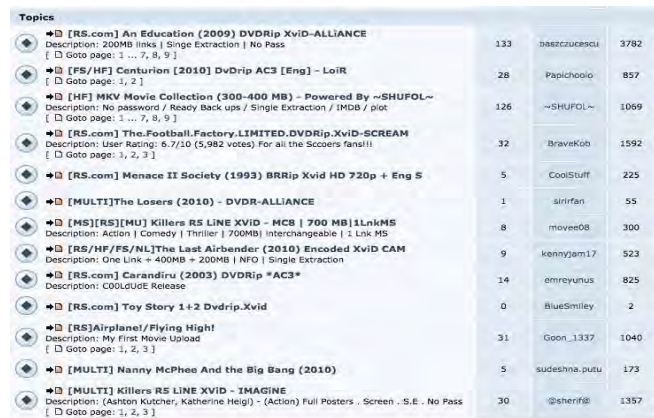
To store or access content on a cyberlocker, users need only a web browser – unlike P2P programs like bittorrent and eDonkey which require a dedicated client application. Also, direct downloading from a cyberlocker can be quicker than P2P on high bandwidth connections, more anonymous than P2P, and is often (at least at present) less prone to malware, viruses, and spoofing.

Users can freely upload any material to such sites and are then provided with a link with which anyone can then access that content. For non-paying users, content remains on the service for a limited period, can only be downloaded a certain number of times, and can only be downloaded after a waiting period of a minute or so while the potential downloader is presented with various advertisements. Premium memberships (typically costing around USD \$13 / €10 a month) allow content to be stored for longer and – more importantly for downloaders – grant those prepared to pay with instant and high speed downloads of any content (not just their own) stored on the service.

Significantly, the vast majority of cyberlockers do not allow the content they hold to be searched in the same manner as a torrent portal: there is no way to query Rapidshare or MegaUpload for every file they hold that matches the phrase 'Lost' or 'Spiderman', for instance. This would seem to limit the attraction of these sites for piracy purposes but, as with many pieces of web-based technology, they were quickly co-opted for the purposes of containing and distributing pirated material. Hundreds of third-party **cyberlocker indexing sites** (such as FilesTube, right) and **link sites** (such as Warez-BB, shown in the screenshot below) have appeared in the last



couple of years which collate and make available links to pirated content held on cyberlockers. A user of such a site uploads a file to Rapidshare or another cyberlocker and then posts the link to that file on one of the many bulletin boards, forums, or indexing sites that cater to cyberlocker users. Any user can then click to obtain the material. As noted above, downloads are free, though users must sit through a wait time before the download can start and speeds are limited *unless* a premium account is purchased – this brings downloads that begin instantly at speeds which are usually as fast as the user's broadband capacity.



Topics			
➡ [RS.com] An Education (2009) DVDRip XviD-ALLIANCE Description: 200MB links Single Extraction No Pass [Goto page: 1 ... 7, 8, 9]	133	baezcuerscu	3782
➡ [FS/HF] Centurion (2010) DvDrip AC3 [Eng] - LoIR [Goto page: 1, 2]	28	Papichooig	857
➡ [HF] MKV Movie Collection (300-400 MB) - Powered By ~SHUFOL~ Description: No password / Ready Back ups / Single Extraction / IMDb / plot [Goto page: 1 ... 7, 8, 9]	126	~SHUFOL~	1069
➡ [RS.com] The Football Factory LIMITED DVDRip XviD-SCREAM Description: User Rating: 6.7/10 (5,982 votes) For all the Soccer's fans!! [Goto page: 1, 2, 3]	32	BraveKoh	1592
➡ [RS.com] Menace II Society (1993) BRRip Xvid HD 720p + Eng S	5	CoolStuff	225
➡ [MULTI] The Losers (2010) - DVDR-ALLIANCE	1	siirfan	55
➡ [MS][RS][MU] Killers R5 LINE XVID - MCB 700 MB 1LnkMS Description: Action Comedy Thriller 700MB Interchangeable 1 LnK MS	8	movee08	300
➡ [RS/HF/FS/NL] The Last Airbender (2010) Encoded Xvid CAM Description: One Link + 400MB + 200MB NFO Single Extraction	9	kennyjam17	523
➡ [RS.com] Carandiru (2003) DVDRip *AC3* Description: COOLGUE Release	14	emryyus	825
➡ [RS.com] Toy Story 1+2 Dvdrip.Xvid	0	Bluesmiley	2
➡ [RS] Airplane! / Flying High! Description: My First Movie Upload [Goto page: 1, 2, 3]	31	Goon_1337	1040
➡ [MULTI] Nanny McPhee And the Big Bang (2010)	5	sudeshna_pu	173
➡ [MULTI] Killers R5 LINE XVID - IMAGINE Description: (Ashton Kutcher, Katherine Heigl) - (Action) Full Posters - Screen - S.E. - No Pass [Goto page: 1, 2, 3]	30	@shenif	1357

Screenshot from WareZ-BB link site

The practice is not as large as bittorrent (and the need to pay for a premium account before the full benefits can be realised is one of the reasons why), though it has grown significantly over the last two years. The largest cyberlockers are among the most popular web sites in the world: for instance, ComScore estimates that



4Shared and MegaUpload have around 78m unique users each month (more than twice as many as ThePirateBay, the largest bittorrent portal); RapidShare 60m unique users; and Hotfile 53m unique users. Alexa ranks 4Shared.com as the 66th most popular site in the world and MegaUpload as the 67th most popular. The usage studies in Part B estimate traffic to web-based cyberlockers and centralised file hosts at around 7% of all internet usage, though this varies significantly from country to country and may be as low as 2.5% for North America and the United States. Sandvine estimates overall usage of Rapidshare and MegaUpload together as 5.1% of all internet traffic.

Methodology

Envisional's Discovery Engine technology (an automated search, identification, and classification system for internet content) was employed to crawl the internet to locate links to content stored on ten large cyberlockers like Rapidshare and MegaUpload. The intention was to locate as many links as possible and then to analyse those

links to see what type of content had been uploaded to the cyberlocker (e.g., a film, television episode, ebook, photograph) and to determine whether that content was likely copyrighted or not.²⁰ A random sample²¹ of 2,000 links gathered by the Discovery Engine was taken and analysed and the content type noted²². The results are below together with the proportion of each found to be copyrighted.

Content type	Links found		Copyrighted	
	#	%	#	%
Films	715	35.8%	709	99.2%
Television	169	8.5%	162	95.9%
Pornography	401	20.1%	345	86.0%
Music	201	10.1%	189	94.0%
Games	187	9.4%	155	82.9%
Software	199	10.0%	180	90.5%
Books / Audio books	52	2.6%	38	73.1%
Other / unknown	76	3.8%	30	39.5%
Total	2,000	100.0%	1,808	90.4%
Excluding pornography	1,599	79.95%	1,463	91.5%

As with bittorrent, much of the analysed content – over 90% – appeared to be copyrighted. The vast majority of films, television episodes, music, software, and games were copyrighted and available on cyberlockers illegitimately.

²⁰ An obvious shortcoming of this approach is the difficulty of finding links to non-copyrighted files legitimately stored on cyberlockers as such use does not generally involve publicizing a link onto the wider internet (personal photos, for instance, would likely be shared with family and friends via an email link). Still, it is reasonable to assume that while cyberlockers such as Rapidshare may host a non-trivial amount of non-copyrighted content, the *popularity* of that content – and hence the number of downloads and amount of bandwidth utilised – is likely limited.

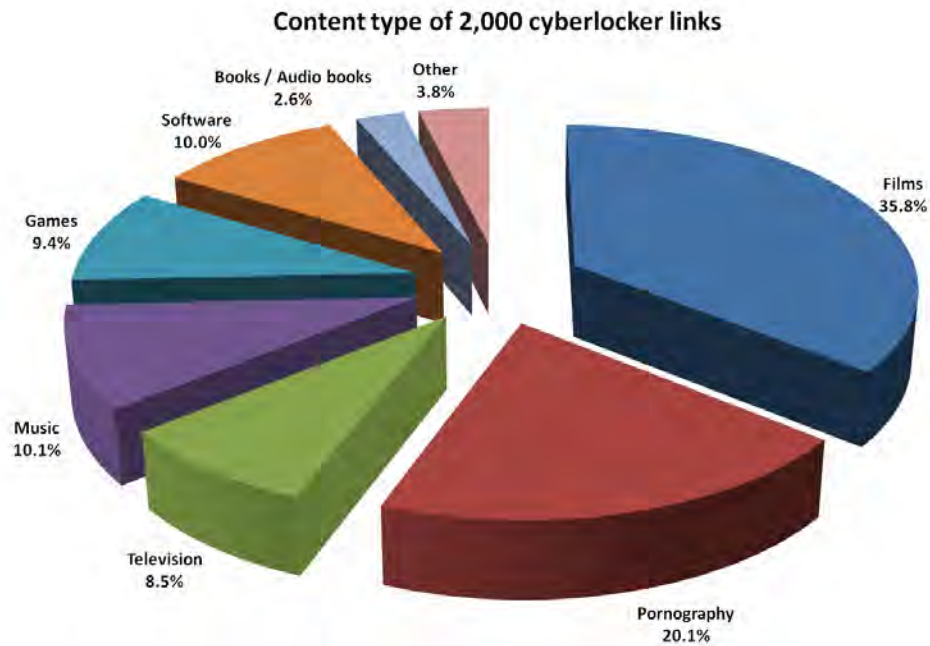
For example, Rapidshare announced a bandwidth upgrade to 600 Gbps (75 GBps) in March 2010 (<http://en.wikipedia.org/wiki/RapidShare>). This enabled a theoretical maximum of 194.4 PetaBytes/month to be transferred. Applying an 80% utilization factor results in an estimate of 155 PetaBytes of content transferred each month. With 50 million unique monthly users of Rapidshare (a figure taken from Google Trends), this amount of content equates to each user of the service downloading 4.15 movies per month. If films were replaced by collections of non-copyrighted photographs, those 50m unique users would need to download 307 collections of photos each month (assuming that each batch of photos comprised forty photos at 250Kb each = 10MB) were Rapidshare's bandwidth to be used entirely by this type of content.

The focus in this example is on downloading for, as Sandvine noted in its 2009 report: "Rapidshare is used primarily for data acquisition (*there is relatively little upstream traffic*) [emphasis added] and is generally not popular with average broadband subscribers." See: <http://bit.ly/sandvine>

The basic fact is that experienced internet analysts and researchers can find very little evidence that the bandwidth consumed by cyberlockers is used in the distribution of non-copyrighted content to any substantial extent.

²¹ The sample was selected using a random number generator.

²² Many cyberlockers only allow files of a particular size to be uploaded. This means that files greater than this size must be uploaded in parts. The common way to do this is to break the larger file into smaller 'Rar' files generated by the Rar archiving tool. The files will typically be named 'Filename.rar' and 'Filename.ra1' or 'Filename.part01.rar' and 'Filename.part02.rar'. When the Rar files are unarchived, the resulting file is re-created. For the purposes of this analysis, a file with multiple parts was treated as being a single file.



There is a larger proportion of smaller files such as eBooks and music on cyberlockers than on bittorrent. This accords with Envisional's experience of how each file sharing method is used. For example, with a cyberlocker, uploading is a simple one-click process that lasts only for the time necessary to upload the full file. There is no long-term uploading relationship and the upload occurs once at the decision of the uploader. Bittorrent, on the other hand, relies on a group of individuals exchanging small parts of a large file and the initial file creation process and upload process takes time and some knowledge. Seeding files is an ongoing process which can require long-term usage of a bittorrent client and an internet connection. Finally, files are uploaded only when and if another individual decides to download the file on offer – an element of uncertainty not present with cyberlockers. All in all, these differences provide cyberlockers with an ease-of-use advantage over P2P and users may respond by uploading a greater number of smaller files such as music and books.

2.5 Discussion: Video streaming

Every recent report which examines the recent past and immediate future of internet usage (see Part B) identifies streaming video as the fastest growing segment of bandwidth consumption worldwide. Led by YouTube, determined by most research to consume at least 5% of all internet bandwidth alone, the use of streamed video has become widespread across the entire internet. Sandvine believe that 'real-time entertainment' (streamed content consumed as it downloads) comprises 26.6% of all internet usage; Cisco state that 'streaming' traffic is 27.8%; and Arbor Networks estimate that 25% of traffic is streamed video or audio of some kind. All studies also cite the significant rise in this segment of internet usage and all predict further growth in this area.



Unlike bittorrent, eDonkey, and cyberlocker usage, experience indicates that most usage of video streaming is benign and poses no threat to copyright: Facebook videos of parties, news reports, YouTube rants, and so on. The rise in video streaming has gone hand-in-hand with the increase in user generated content pushed onto the internet and it is obvious to anyone with a passing familiarity with sites like YouTube that the majority of content currently uploaded onto such sites is produced by users and is not copyrighted or is uploaded legitimately by content owners (for instance, of the top ten 'most viewed' videos on YouTube, six are legitimately-uploaded music videos totalling 850m views).

However, there can also be no question that there is a significant amount of pirated content available which has been uploaded to video hosting sites across the world. There is an obvious appeal to internet users of films and television episodes which begin seconds after a user clicks play rather than requiring a wait for the download to complete before consumption. Browser-based and easy-to-use, video streaming web sites are a major concern of content owners and it is not difficult to find pirated versions of any major film or television series with a few minutes of persistence.



YouTube itself prevents most users from uploading content longer than fifteen minutes in length and has added tools such as digital fingerprinting to ensure that copyrighted material is identified and banned but the site has been host to a broad section of unauthorised copyrighted material in the past. Other video hosts are often much

less willing to implement proactive barriers to pirated content, allowing longer-duration uploads while enabling high quality streaming and refusing to implement filtering for copyrighted material.

In a similar fashion to the way that cyberlocker link sites have co-opted cyberlockers for piracy purposes, so video link sites have done the same for video hosts. Sites such as **LetMeWatchThis** and **Movie2k** index pirated content held on video hosts to present users with numerous choices for the latest film or television show. For instance, LetMeWatchThis currently offers forty-three separate working links to view *Inception* on different video hosting sites. Video link sites either embed Flash-based video players which stream content hosted on sites like MegaVideo or directly link viewers to the hosts that contain the streaming video.



Streaming videos of pirated content can also be found using a normal search engine. For example, querying Google for terms such as 'watch toy story 3 online' reveals a plethora of linking sites and blogs in the top ten results which offer links to streams of unauthorised pirated versions of the film.



The most popular piracy video link sites gather millions of visitors each month. ComScore estimate LetMeWatchThis to have 6.5m unique users each month and Movie2K to have 5.0m unique users, for example.

Estimating pirated usage of video streaming

Estimating the amount of total video streaming bandwidth that may be unauthorised copyrighted material is difficult. Unlike bittorrent, where the PublicBT tracker manages millions of separate swarms, there is no major repository of video which can be taken to provide a good overall indicator of total video use: YouTube is certainly dominant in this space but as mentioned, there are a number of factors which ensure that YouTube is currently minimally used for new pirated content. The widespread nature of video use across the web means that a link analysis as performed for cyberlockers would be unlikely to gather accurate data.

After reviewing a number of possible methodologies, the best approach to this difficult area was deemed to be one which compared the popularity of index sites used to locate streaming pirated content with index sites used to locate pirated material available via bittorrent.

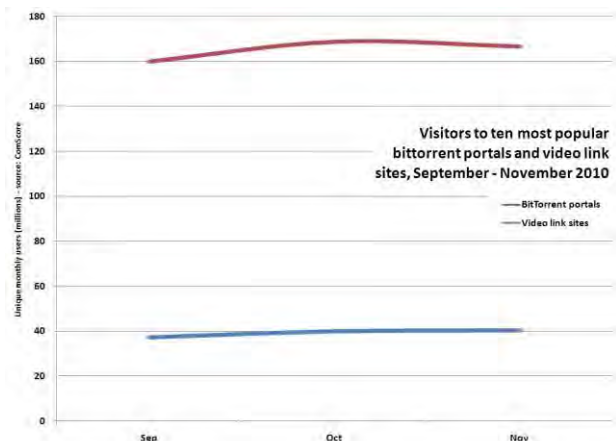
Web metric providers such as ComScore and Alexa offer statistics on the number of daily or monthly visitors to bittorrent portals such as ThePirateBay, IsoHunt, and Torrentz, the main sites from which the vast majority of bittorrent users find links to the pirated content that they ultimately download using the bittorrent protocol – and which then results in the large amount of bittorrent traffic seen in the usage studies. In the same way, users of video streaming sites use portals such as LetMeWatchThis, ZMovie (right) and Movie2K to locate links to pirated content they wish to see, clicking through to the video hosts where the content is hosted. By comparing the known audience for bittorrent portals with the known audience for video link sites, a rough estimate of pirated usage may be possible.



ZMovie

Both types of sites – bittorrent portals and video streaming link sites – are almost entirely devoted to pirated content: scans of the content available on bittorrent sites like ThePirateBay and IsoHunt and video link sites such as LetMeWatchThis and TVShack find close to no content which is not copyrighted (and that this content is unpopular when and if it does exist). It can then be broadly assumed that visitors to video streaming link sites will be consuming pirated material.

The chart shows data from ComScore for monthly unique users to the top ten bittorrent portals and the top ten video link sites worldwide from September to November 2010. Clearly, bittorrent is a much more popular activity on this measure: on average across these three months, the top ten video link sites had an audience just under one-quarter (23.71%) that of the top bittorrent portals – or to put it another way, the



Copyright © 2011 Envisional Ltd

piracy.intelligence@envisional.com

bittorrent portals had slightly over four times as many visitors (4.22x).

Assuming that the end result of a visit to a bittorrent portal is the same as a visit to a video streaming link portal – that a user locates and downloads or streams the content in which they are interested – then the total data which is then transferred must be considered. The amount of data required to consume a file via a video streaming site is usually significantly less than when downloading a film or television episode from bittorrent. The file size is usually much smaller (and hence the final quality of what the user views is often poorer – which may be one reason why bittorrent is more popular as it provides higher quality content).

For example, each link for the ten most recent films posted to a popular video linking site was analysed and the streaming file to which it pointed on a video host was measured in terms of file size. On average, the streamed content comprised 384.2MB. Data taken from the analysis of PublicBT earlier in this report found that the average file size for downloaded films was 937.7MB. On this estimate, it means that each film downloaded via bittorrent results in almost 2.5 times (2.44x) as much data for the same content as via video streaming (or, stated another way, consuming a film via video streaming results in less than half the network traffic (40.97%) as downloading it via bittorrent).

$$\frac{\text{Visitors to Video Link Sites}}{\text{Visitors to Bittorrent Portals}} \times \frac{\text{Streaming File Size}}{\text{Bittorrent File Size}} = \text{Ratio of streaming traffic to bittorrent traffic}$$

As such, video link site traffic may generate the amount of data equivalent to **9.71% of all bittorrent traffic** (video link site visitors as a proportion of bittorrent portal visitors divided by the difference in average file size consumed). The detailed calculation is shown below which, assuming that Sandvine's estimate of bittorrent traffic is correct (14.56%), finds that the traffic which comes from video link sites that link to pirated material is equivalent to **1.42% of all internet traffic**.

A. Amount of all internet traffic measured as bittorrent (Sandvine) ²³	14.56%
B. Amount of all internet traffic measured as video streaming of any kind (average estimate from Sandvine, Arbor, and Cisco – see Part B of this report)	26.5%
C. Video link site visitors as a percentage of bittorrent portal visitors	23.71%
D. Average streamed file size from video link sites (384.2MB) as a percentage of average film file size downloaded via bittorrent (937.7MB)	40.97%
E. Estimated pirated data usage of video link sites as a percentage of all bittorrent internet traffic (C * D)	9.71%
F. Estimated pirated data usage of video link sites as a percentage of <i>all</i> internet traffic (A * E)	1.42%
G. Estimated pirated data as a percentage of all streaming traffic (F / B)	5.34%

Given the difficulty of gathering data in this area, these figures should be taken as a cautious estimate.

²³ Sandvine estimates bittorrent traffic to be 14.56% of total internet usage and is the only company to provide a figure specifically for bittorrent based on a large amount of data – Ipoque did estimate bittorrent usage but its estimate is based on a small amount of total data from a low number of monitoring sites. Other companies talk of “peer-to-peer” usage and not “bittorrent usage”.

Also, Sandvine measured peer-to-peer usage as a lower proportion of all internet usage than some other providers (particularly Cisco) leaving open the possibility that bittorrent usage may be higher. As Sandvine are the only company to provide data for bittorrent alone, their estimate will be used but should likely be taken as a minimum.

2.6 Discussion: Other file sharing arenas

Analysis was also made of three other file-sharing arenas where copyrighted content is generally distributed: eDonkey, Gnutella, and Usenet.

2.6.1 eDonkey

The eDonkey peer to peer network is one of the oldest peer-to-peer networks still in existence. It is heavily used in mainland Europe (particularly in Spain, Italy, and France). Envisional measure between 2.5m to 3m users simultaneously connected to the network or a decentralised network overlay for the network called Kad. Sandvine estimates eDonkey traffic at 1.5% of all internet usage globally.

The most accurate way to calculate the proportion of pirated material available on eDonkey would be through analysis of one or more eDonkey servers and the content which is indexed and downloaded. However, such servers are high priority targets for anti piracy organisations and would be unlikely to cooperate with a request for oversight of the content which they have indexed. While it is possible for anyone to establish a server, doing so helps facilitate the distribution of content between users connected to that server and with much content felt to be pirated, this was not deemed to be a suitable way to research this area.

Instead, searches were made using the eMule client and Envisional's own peer-to-peer monitoring technology for one hundred pieces of content for which results would likely be pirated (new films and television episodes, for instance) and one hundred pieces of content for which results would not be pirated (content legitimately allowed to be distributed such as live concerts from some artists and books licensed under Creative Commons).²⁴ In each case, the most popular instances of each content type were chosen. The number of complete sources for each piece of named content were counted.

The amount of legitimate content available amounted to **1.2%** of all the content located on the network. This is a tiny proportion and while the research is not methodologically perfect, it does indicate that the majority of material held and transferred on eDonkey (in this analysis, **98.8%**)²⁵ is likely copyrighted.

²⁴ For example, copyrighted film content such as *The Dark Knight* and *Avatar* and television episodes from series such as *Lost*, *Heroes*, and *Doctor Who* and non-copyrighted material such as live concerts from Pearl Jam, books licensed under Creative Commons such as Cory Doctorow's *Makers*, and films like *Steal This Film*.

²⁵ Though this figure excludes pornographic content for which searches were not made.

2.6.2 Gnutella

The Gnutella network is widely used for the distribution of music as well as other content. Envisional's own Gnutella crawler estimates the network to have around 2.0m users at any one time since the closure of the company behind the LimeWire client at the end of 2010. Sandvine estimates Gnutella usage at 1.9% globally and the network is particularly popular in North America.

Envisional analysed the searches made by users on the network²⁶. A sample of 3,500 search queries were examined for the content type to which they most likely referred and as to whether the content sought was copyrighted or not²⁷. The table below shows the results. The 'copyrighted' column only includes those queries for which the copyright status could be clarified.

Content type	Search queries		Copyrighted	
	#	%	#	%
Film	144	4.12%	144	100.00%
Television	254	7.26%	254	100.00%
Pornography	453	12.95%	Unknown	Unknown
Games	59	1.69%	53	89.90%
Music	1,920	54.87%	1,786	93.00%
Other	108	3.11%	105	96.70%
Unknown	560	16.00%	Unknown	Unknown
Total	3,500	100.0%	2,342	66.9%
Excluding pornography and unknown	2,487	71.06%	2,342	94.2%

It was not possible to determine the copyright status of the pornography for which users searched. A large section of 'unknown' queries included many queries in Japanese (around one-fifth of all unknown queries) which could not be accurately translated. However, a majority of such Japanese queries for which translation was possible indicated that the search was likely for a pornographic video of some kind.

While it seems clear that music content is the most popular on the network – a finding supported by other research into Gnutella – there are some obvious methodological issues with using this process to calculate copyrighted content. For instance, search queries do not necessarily translate into downloads, particularly if the query cannot be matched exactly. Nonetheless, it is telling that 94% of the non-pornographic searches that could be identified were for copyrighted material. A similar study by Professor Richard Waterman of the University of

²⁶ Clients which act as 'supernodes' receive search queries from other peers on the network and other supernodes.

²⁷ For instance, a search for 'Lady Gaga telephone' was assumed to be a search for the audio version of this song. A search for 'Lady Gaga telephone video' or 'gaga video' was assumed to be looking for a music video. A search for 'telephone' could not be classified as any particular content type and was thus categorised as 'unknown'.

Pennsylvania which used a sample of 1,800 files found that 98.8% of files requested on Gnutella were either copyrighted or highly likely to be copyrighted.²⁸

2.6.3 Usenet

Usenet is one of the oldest communications arena on the internet – and as with many areas of the internet, the system was quickly co-opted by those wishing to spread pirated content after its initial appearance. A few years ago, a small web site (recently shut down after legal action in the UK²⁹) created the ‘NZB’ system for quickly retrieving large files from Usenet. NZB files opened up Usenet to a much larger potential audience and offered third-party services an opportunity to create businesses centred around facilitating access to Usenet. Some of these businesses, such as Usenext in Germany, are now multi-million Euro operations (Usenext had revenue of €30m in 2007). Significantly, almost all committed Usenet users pay for access: Usenext charge between €10 and €25 Euros per month and similar services do the same. The necessity to pay for access to Usenet has certainly limited the spread of the system as a way to obtain pirated content but Envisional believes that up to half a million users connect regularly to Usenet to obtain pirated content³⁰. The usage studies cited in Part B that look explicitly at Usenet estimate overall traffic devoted to the arena at between 0.5 – 1% of overall internet usage.

Usenet began as a text-based medium meant for sending simple text messages. This remains the only real use for the system outside of transmitting files and it is unlikely that this aspect of the service takes up more than a tiny percentage of overall Usenet usage. In order to determine usage of Usenet for the transmission of copyrighted material, a random selection of 100 newsgroups from the many thousands available through the Giganews Usenet provider³¹ were sampled and the last 100 complete files or messages posted to each newsgroup analysed. The copyright status of each post was checked. Text messages made up 3.2% of all posts; **93.4% of all posts** (all of which were files) contained copyrighted content; 2.3% were likely copyrighted; and for 1.1% of posts (all files), the copyrighted status could not be identified.

Thus at least 93.4% of sampled posts made to Usenet contain copyrighted content. However, given the size of these files (for instance, a typical film posted to Usenet will be at least 700MB in size), each post containing copyrighted content will dwarf the size of any text posts made. In terms of the actual amount of data transferred over the network, copyrighted material likely makes up more than the 93.4% of individual posts.

²⁸ See <http://www.scribd.com/doc/31284309/Arista-et-al-v-Lime-Wire-et-al-summary-judgment>.

²⁹ <http://newzbin.com/>

³⁰ An estimate made by reference to the amount of traffic received by major Usenet providers and NZB sites as well as through analysis of the published accounts of a large Usenet access provider in Europe.

³¹ <http://giganews.com/>

3 Part B: Internet Usage Assessment

3.1 Introduction

This part of this research report critically evaluates recent research produced by a number of companies that offer different pictures of overall internet usage. Four main studies of bandwidth usage were examined. Each study was released during the second half of 2009 and were conducted by four network monitoring companies, mostly using data gathered during 2009:

- Sandvine Incorporated
- Arbor Networks
- Cisco
- iPoque

Each of the studies had the same broad aim: to illustrate the protocols and applications which are used across the internet and to show how much of the internet's bandwidth is used by each. For instance, each study analysed the amount of internet traffic taken up by peer to peer technologies or by streaming video as well as more traditional pursuits such as normal web browsing and email. However, direct comparison between each was problematic.

Each study:

- used different monitoring techniques
- was based on varying periods of time, examined different amounts of data and looked at different areas of the world
- used different categorisations for types of traffic

The categorisation issue is one of the largest problems with comparing the four studies. For instance, all four studies identify streamed video as a growing portion of internet traffic. However, each study uses a slightly different method of identifying this traffic and sometimes include the content in a different broad category which also comprises other items. For instance, Arbor Networks uses the simple term 'Video' to mean progressive video downloads; Sandvine speaks of 'Real-time entertainment' to denote video and other content such as audio which is consumed as it is downloaded or streamed; Cisco classifies 'Internet video to PC' as video or television on demand viewed on a computer; while iPoque uses the category 'Streaming' to refer to any kind of streamed audio and video. Some categories appear to be fairly consistent across all four studies: for example, all use 'P2P' as a broad identifier for known peer to peer networks. However, it was not always possible to determine the range of peer to peer networks detected by each monitoring company (though the largest known networks such as bittorrent, eDonkey, and Gnutella seemed to be always included), nor to know their rate of successful detection.

None of the four studies can be accepted without reservation, though some offered more confidence than others. The following sections discuss each of the four studies in detail, outlining the main points, the basis of the findings, and the methodological issues which are attached to each of them.

3.2 Sandvine: 2009 Global Broadband Phenomena

Monitoring period: September 1st – 22nd 2009

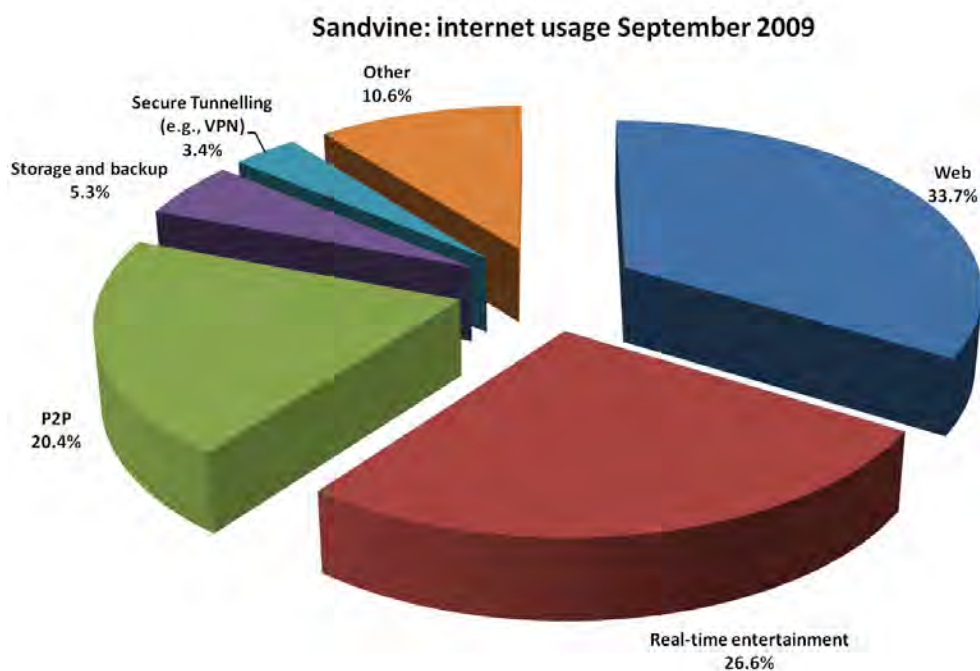
Monitoring locations: 22 ISPs in five regions: nine from North America, five from Europe, four in the Middle East and Africa, two in the Caribbean and Latin America, and two in Asia-Pacific

Number of subscribers: 24 million.

Amount of traffic monitored: Unknown

P2P traffic: 20.4%

Streaming video traffic: 26.6% (categorised as 'real-time entertainment' – content consumed as it is downloaded)



Other points:

- 'Storage and backup' services (which include cyberlockers and web-based backup services) consume 5.3% of internet traffic
- P2P proportion is 18.5% in North America
- Streaming video proportion is 26.7% in North America
- 'Real-time entertainment' category (streamed or buffered video or audio) more than doubled from 12.6% in 2008 to 26.6% in 2009.
- Significant variation between regions

3.2.1 Methodology

Sandvine is a Canadian-based network monitoring provider. The company's 2009 *Global Broadband Phenomena* report repeated analysis completed in 2008. The study contained a detailed categorisation of content and thorough analysis of current trends based on 24 million subscribers from twenty ISPs in five regions, including nine ISPs located in the United States. Their data is based on internet traffic flowing through Sandvine's monitoring equipment and captures application usage from the subscriber's perspective. The company is also able to detect visitors to some popular web sites (such as YouTube and Rapidshare). Analysis looks at the average subscriber in a number of regions across the world and also uses a weighted global average of data to provide overall figures.

The main finding of the Sandvine study is the identification of a *"dramatic shift' from bulk download 'experience later' behaviour towards real-time 'experience now' application"*. Sandvine uses a category termed 'Real time entertainment' to denote streamed video or audio which is consumed as it is downloaded. In 2009, this category accounted for 26.6% of total traffic, an increase from 12.6% in 2008. The increasing consumption of video content by internet users is a common theme within most of the studies.

Sandvine issued a 2010 *Global Broadband Phenomena* update as this Envisional report was being finalised. The 2010 report³² did not provide data for worldwide traffic but found that 'real-time entertainment' continued to grow, accounting for up to 43% of peak time traffic in North America (with Netflix measured at 20% of peak time downstream traffic alone). Peer to peer traffic remained very important: bittorrent was found to comprise nearly 17% of downstream traffic during peak periods in North America and 37% in Latin America.³³

3.2.2 Discussion

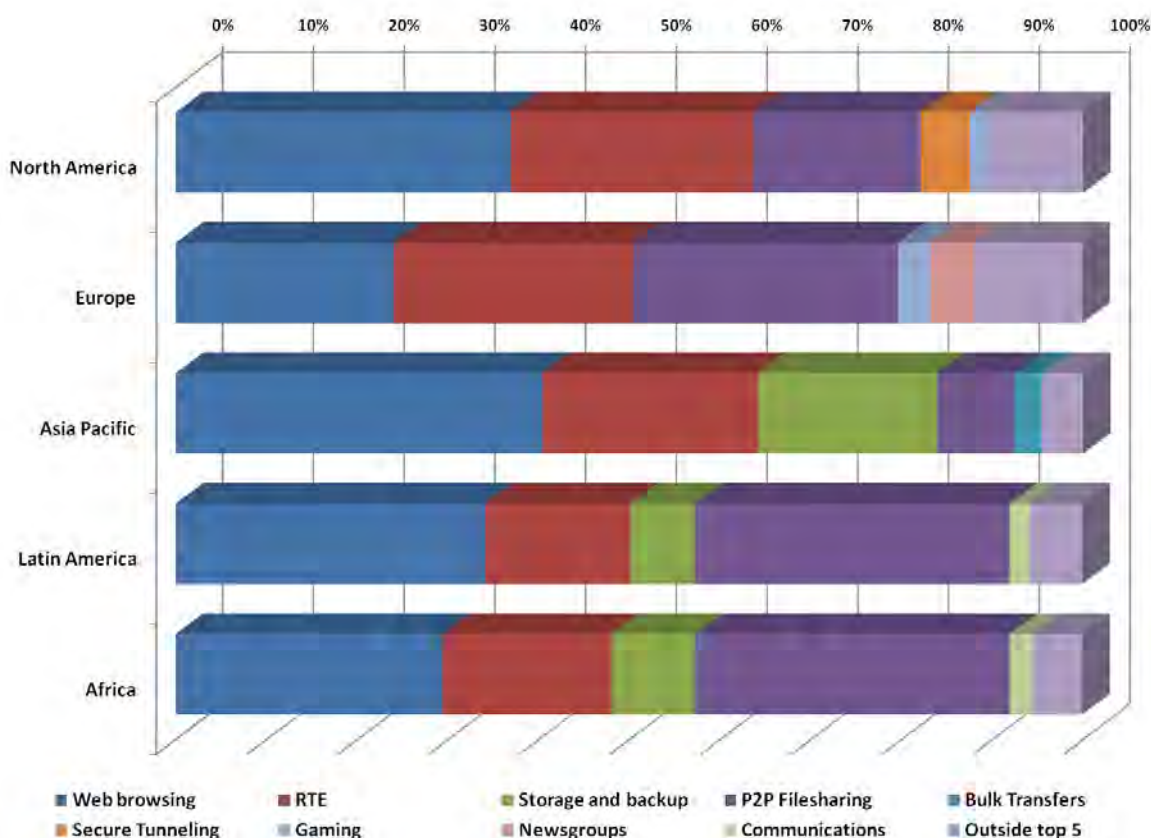
The chart on the page above illustrates the top five categories in terms of traffic detected worldwide by Sandvine. Web surfing contributes just over one-third (33.7%) of all traffic with the 'Real-time entertainment' (RTE) category responsible for more than one-quarter (26.6%, more than doubling in size since 2008). While much of this activity takes place through the web or browser it is separately categorised by Sandvine. Peer to peer filesharing then adds a further one-fifth (20.4%) of all traffic. More than 80% of internet traffic is thus taken up by these three categories alone. A 'storage and backup' category refers to cyberlocker sites such as Rapidshare which allow centralised file hosting and retrieval via the web (and which are often used for piracy purposes).

³² http://www.sandvine.com/news/global_broadband_trends.asp

³³ There are some areas in which the 2010 report raises questions - for instance, in highlighting Zshare as the most popular cyberlocker in Europe. All other information gathered by Envisional from our own and other data sources cite Rapidshare, Hotfile, and MegaUpload as the three most-used cyberlockers with Zshare a second- or even third-tier site. For instance, data from ComScore place Zshare as the eighth most popular cyberlocker with one-tenth of the number of visitors of the most popular site.

Sandvine's report also makes clear that internet usage varies greatly across the world, a theme that is repeated in the reports from Cisco and iPoque. The chart below shows the top five categories of traffic in the different monitoring regions used by Sandvine. Some of the main differences are as follow:

- Web browsing as a portion of internet traffic ranges from 24% in Europe to 40% in Latin America
- P2P usage ranges from 8.6% in the Asia Pacific region to 34.7% in Africa
- Storage and backup services (online file hosts) are under 1.9% of internet usage in North America but 19.7% in Asia Pacific (influenced by the heavy use of centralised 'web-hard' services like PDBox in Korea, a location where Sandvine have monitoring equipment installed)
- Gaming traffic is (just) one of the five largest categories in North America and Europe but nowhere else.
- Newsgroups provide 4.7% of traffic in Europe but do not appear in the top five in any other region.
- Real-time communications traffic appears in the top five categories for Latin America and Africa but not elsewhere.

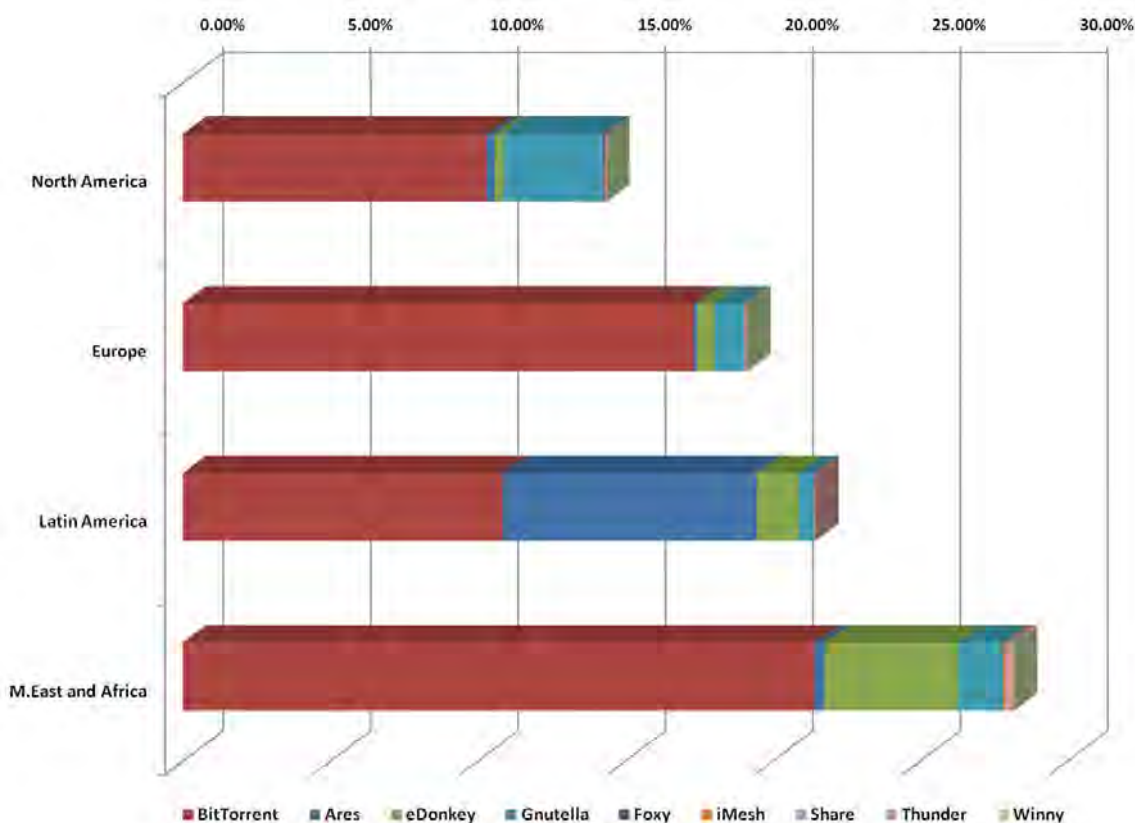


3.2.3 Additional detail

Sandvine provided Envisional with further detailed information on traffic from individual P2P applications as well as a small number of central web sites³⁴. This additional data was broken down by four regions.

Sandvine tracked nine P2P applications: BitTorrent, eDonkey, Ares, Gnutella, iMesh (a client that connects to a legitimate music network), and four clients predominantly used in Asia: Foxy (a variant of Gnutella), Share and Winny (two popular Japanese networks), and Thunder (a download manager / P2P application popular in China where it is usually known as 'Xunlei'). Absent are some well-known protocols such as Shareaza and DirectConnect. It is unknown whether Kad, the decentralised sister network to eDonkey, was classified under the eDonkey header. (Peer to peer television (P2P TV) clients such as PPLive and PPStream are classified as 'Real time entertainment'.)

The chart below shows the percentage use of these P2P networks in each of the regions examined by Sandvine. Again, usage differed from region to region. The data is the average downstream usage of each application.

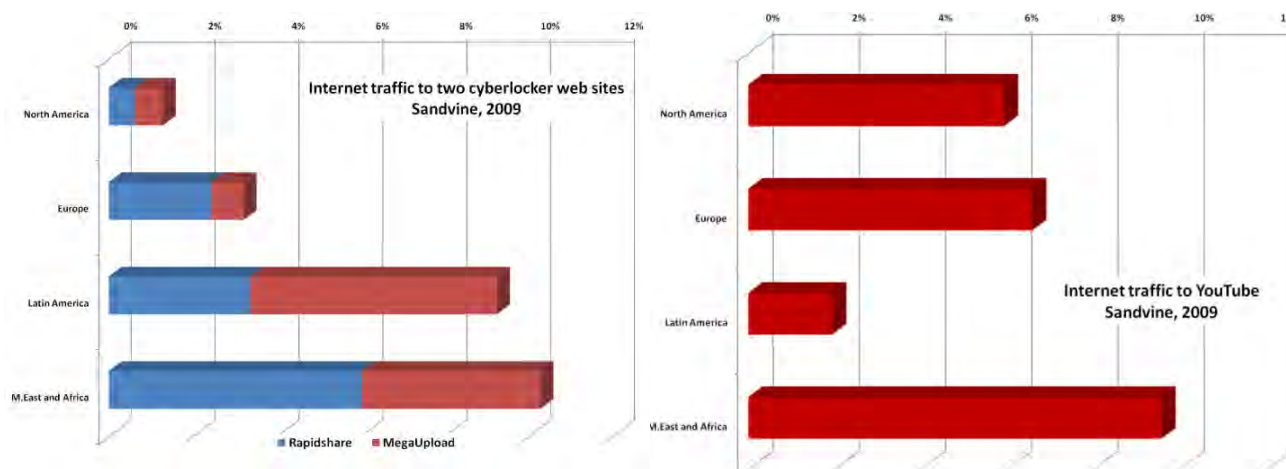


³⁴ Envisional is grateful to the author of the Sandvine study for supplying this additional data.

It is clear that BitTorrent dominates the peer to peer world in the locations monitored by Sandvine: the network makes up more than half of all peer to peer usage detected by Sandvine in each of these four regions and almost all in Europe. There is little eDonkey usage apart from in the Middle East and Africa. This finding likely reflects the countries in which Sandvine has monitoring locations in Europe: eDonkey is believed to be well used in many European countries such as France, Spain, and Italy and it would be difficult to believe that the network is responsible for just 0.3% of internet traffic in these such countries. Ares contributes over 8.6% of traffic in Latin America³⁵ while the four Asian clients comprise no more than 0.3% of all internet traffic in any of the four regions (unsurprising, as data was not supplied for the Asia-Pacific region).

- In **North America**, bittorrent (10.3%) and Gnutella (3.4%) make up almost all of the P2P proportion of overall internet traffic of 14.4% (the lowest of the four regions).
- 90% of P2P use in **Europe** is through bittorrent with the network making up 17.3% of all internet traffic in the region and Gnutella contributing a further 1% of all traffic. As noted above, eDonkey usage is believed to be higher in Europe than shown by Sandvine: other estimates place it at 3-5% of internet traffic.
- **Latin America** also sees more bittorrent usage than any other peer to peer application but Ares comprises 8.6% of internet traffic and 40% of all P2P traffic.
- BitTorrent contributes more to overall internet traffic (21.4%) in the **Middle East and Africa** than anywhere else while there is more P2P use (28.2% of all traffic) in this region than any of the other locations monitored by Sandvine, with eDonkey contributing 4.5% to all internet traffic.

Sandvine also supplied data to Envisional on visitors to the two most popular **cyberlocker web sites**: Rapidshare and MegaUpload. In the North America locations, 1.3% of downstream internet traffic was visits to one or another of these sites (MegaUpload was slightly more popular); in Europe, the figure was 3.2% of total downstream traffic (with Rapidshare much more popular); in Latin America, 9.3% of traffic went to these two cyberlockers (that is more traffic than used by the Ares application and almost as much as bittorrent); while in the Middle East and Africa, these two sites alone were responsible for 10.3% of all downstream internet traffic (with Rapidshare contributing 6% of all internet traffic alone).



³⁵ Including the Caribbean.

Across all four regions, these **two cyberlocker sites alone comprise 5.1% of all downstream internet traffic**. To put this into perspective, it is only a little less than the 6.2% of internet traffic consumed by YouTube worldwide, recognised by Sandvine (and Arbor) as the largest single domain contributor to overall internet traffic. As the second chart above shows, traffic to YouTube also varied from region to region, ranging from 1.9% in Latin America to 9.6% in the Middle East and Africa.

3.2.4 Summary

Sandvine's study shows a good level of detail and accompanying analysis. The company's willingness to discuss their approach and provide additional data upon request demonstrates their confidence in the methodology and figures.

However, it is important to remember the relatively small number of monitoring locations from which the data is drawn for some regions (only two locations for Latin America, Asia-Pacific, and the Middle East and Africa) as well as the fact that an overall figure for the amount of data analysed in the study could not be obtained. Further, analysis took place in September, a month when there are few major film releases and the Fall television season in the United States (which tends to produce an increase in the use of P2P networks to download content) is yet to properly begin.

3.3 Arbor Networks: ATLAS Observatory 2009 Annual Report

Monitoring period: July 2007 – July 2009

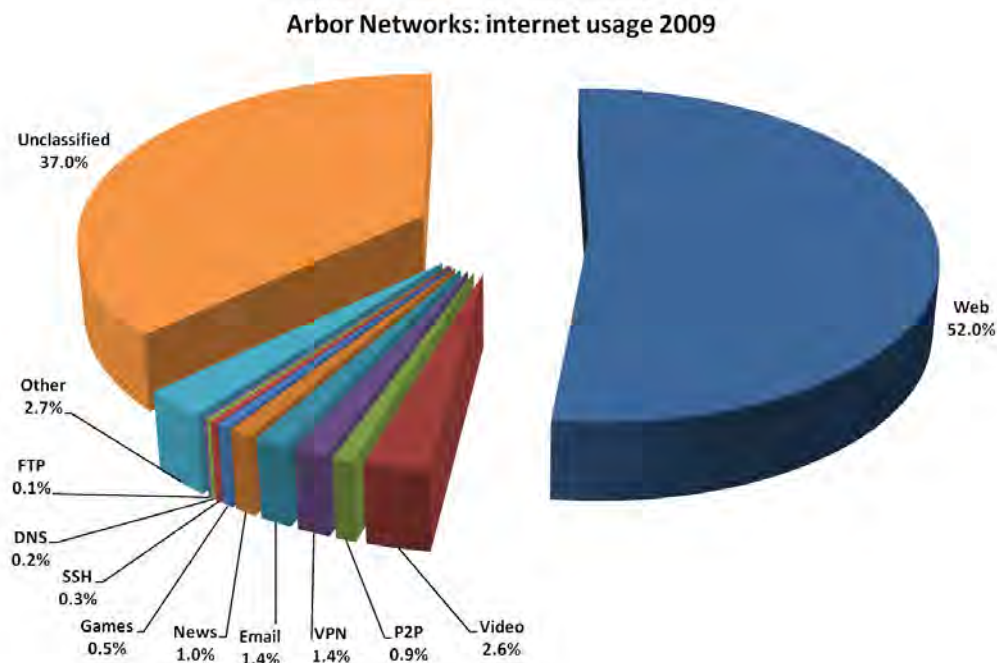
Monitoring locations: 110 deployments across ISPs and Content Providers worldwide (with an emphasis on North America, Europe, and East Asia (including Japan)).

Number of subscribers: unknown.

Amount of traffic monitored: 264 Exabytes of data at a peak rate of 14 Terabytes per second. On average, 9 Exabytes per month. This is by far the largest of all the studies³⁶.

P2P traffic: 0.85% (inspected by port number); 18% (payload inspection of a smaller dataset from 5 ISPs)

Streaming video traffic: 2.64% (estimate of 25% on payload inspection of same smaller dataset)



Other points:

- Streaming video is the fastest growing internet traffic category.
- Google (including YouTube) accounted for 5.5% of all internet traffic in May 2009.
- MegaUpload (a large 'cyberlocker' file host) accounted for at least 0.5% of all internet traffic in May 2009.
- Game console traffic accounted for 0.6% of all internet traffic in May 2009.
- Annual internet traffic growth of 44%.

³⁶ 264 Exabytes = 276m Terabytes = 283bn gigabytes = 64 billion DVDs.

3.3.1 Methodology

Arbor is an established network monitoring and security company. The company's monitoring study is produced in collaboration with authors at the University of Michigan and uses a number of monitoring locations worldwide that employ Arbor's network equipment. These servers sit on the edge of an ISP's network and categorise traffic as it passes with an 'anonymous XML file' containing data reports then sent to central analysis servers.

The Arbor study examines an extremely large amount of content data over a two year period – by far the most substantial data base of any of the four studies. The 264 Exabytes of data is equivalent to 283,500,000,000 Gigabytes – around 64 *billion* full-sized DVDs. The data is taken from a wider spread of monitoring points than others (110, compared to 20 for both the Sandvine and Cisco analyses and just 11 for the iPoque study). A precise breakdown of traffic by region is not outlined but monitoring appears to mainly use locations in North America, Europe, and East Asia (including Japan).

3.3.2 Discussion

The chart above shows the dominance of web-based communication: over half of all internet traffic identified by Arbor took place through the web. Against that, no other identified category was responsible for more than 3% of internet traffic. The video and P2P categories amounted to 3.5% in total.

However, the study is hampered –as the large orange 'Unclassified' segment on the chart makes clear – by issues with detection. In 2009, **37% of the 264 Exabytes of traffic could not be classified** by Arbor. This represents an enormous amount of traffic which could not be identified by the routine monitoring techniques employed by the company. According to subsequent analysis by Arbor, the majority of this unclassified proportion is believed to be either peer to peer traffic or video streaming and downloads, a belief based on analysis of a second and smaller dataset of traffic subjected to more detailed probing.

This second, smaller, dataset was taken from **five consumer ISPs** based in the United States, Canada, Europe, and Asia, though the precise locations and number of subscribers represented are not supplied, and nor is the actual amount of data analysed. This dataset was subjected by Arbor to Deep Packet Inspection (DPI) techniques in an attempt to detect traffic based on the payload of the data. Arbor are confident that their DPI detection is accurate, but detection of peer to peer protocols is not their core business and as such, they may not be catching as much of this traffic as some other companies – certainly, it might be expected that they under-measure P2P than over-measure. However, Arbor were clear in conversation that observations show that there is broad correlation between the overall trends from the smaller DPI-based analysis and the larger, main dataset though without detailed analysis of the smaller dataset this is not possible to confirm.

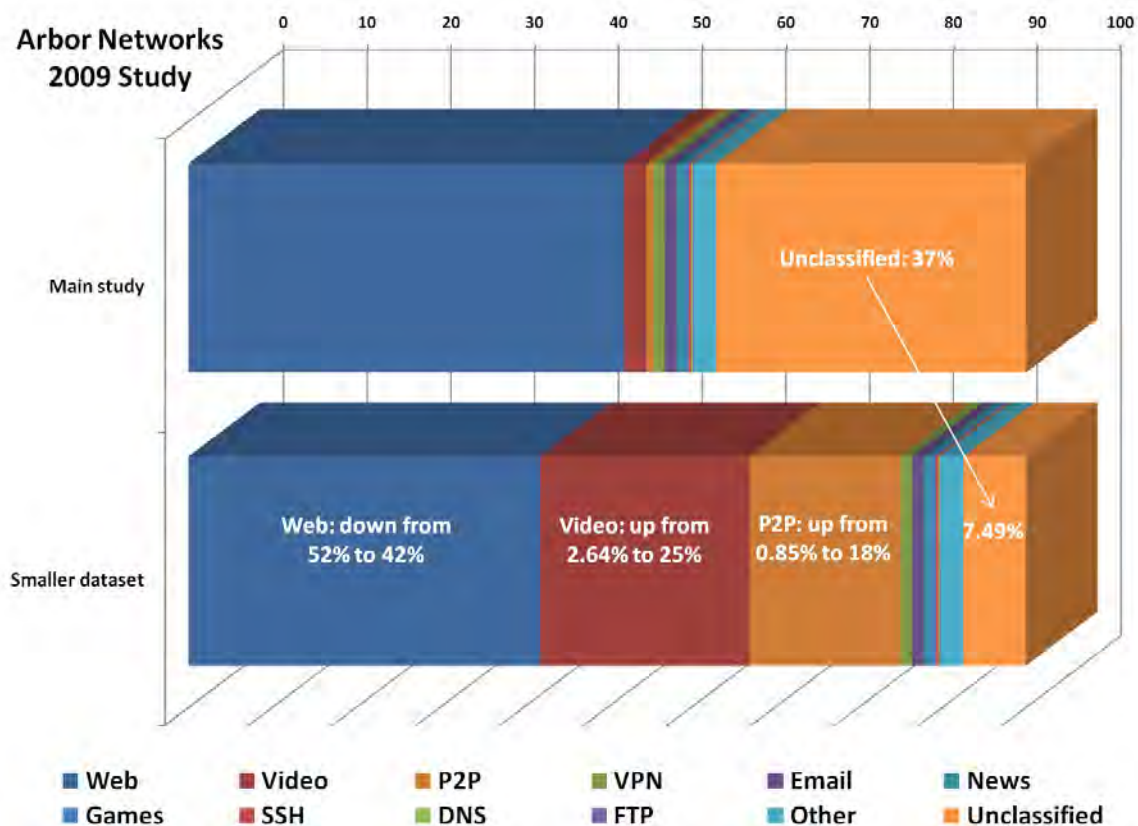
The deeper analysis of the second and smaller dataset via DPI led Arbor to conclude that **"P2P is likely closer to 18%"**. This wording is imprecise and there is no attempt to break down P2P usage by protocol or by region, as

Sandvine manage, for instance³⁷. The dataset was taken from the midpoint of the monitoring (assumed to be during 2008) and no further information is provided on additional changes to P2P traffic after that point.

Similarly, the larger main study appeared to base its analysis of video traffic on older protocols and did not account well for the enormous growth of other transmission methods. A second estimate is made by Arbor through similar DPI analysis of the smaller dataset which estimated video traffic at “**25%+ of all traffic (including 10% of HTTP)**”. Again, the wording is vague and slightly confusing, drawing part of the HTTP traffic to make up the total video proportion.

3.3.3 Accounting for the unidentified data

As noted, **37% of traffic** from the main study was unidentified in 2009. The smaller dataset placed **P2P** usage at 18% rather than 0.85% in the main study, which might account for 17.15% of that unidentified block – leaving 19.85% of unidentified traffic. Some of that may also be accounted for by the **video** data identified by the smaller dataset.



³⁷ The authors do state that P2P varies by region and type of network but this is not elaborated upon.

The smaller dataset identified 25% of data to be video traffic rather than 2.64% in the main study, a difference of 22.36%. However, that figure of 25% for video includes 10% of previously identified HTTP traffic, leaving 12.36% of traffic which can be taken from the unidentified block of traffic.

So if the assumption is made that the smaller dataset portrays similar overall usage patterns to the larger study (and there must obviously be reservations about doing this, given the smaller amount of data and lower regional coverage), calculations then leave **7.49% of traffic unidentified** (37%: 17.15% identified as P2P – 12.36% identified as video).

The chart above shows how the overall usage pattern from the main study significantly changes if the classification of video and P2P usage by the smaller dataset is accepted as correct. While the smaller categories of use (such as email and FTP) remain the same, the three major categories of identified use from the smaller dataset (web, video, and P2P) show large differences.

It is possibly only to speculate what the remaining 'unidentified' amount of traffic might be: given Arbor's primary focus on network monitoring and security, it is possible that some of this data may be peer to peer or other file sharing traffic. Arbor do not mention protocols like those behind 'P2PTV' applications such as PPLive and Sopcast that are often used for video distribution in Asia in their reporting and these may also make up some of the unidentified proportion.

3.3.4 Summary

In summary, the Arbor study, while clearly based on a vast treasure trove of data, is affected by the large amount of that treasure which could not initially be classified. Additional DPI inspection of a smaller dataset provided some additional insight but it is only rational to accept the figures provided for P2P and video consumption in particular as a broad estimate of data usage online rather than a more exact representation.

The issues involved in estimating P2P and video traffic must also affect confidence in figures for the other categories of traffic – although as many of these categories will have changed little over time (for instance, web-based transmissions, email, FTP, and VPN traffic are well established), detection and categorisation should be easier.

3.4 Cisco: 2009 Visual Networking Index Usage Study

Monitoring period: Third quarter of calendar year 2009

Monitoring locations: Over 20 service providers, mostly consumer-based ISPs.

Number of subscribers: 1m

Amount of traffic monitored: Unknown.

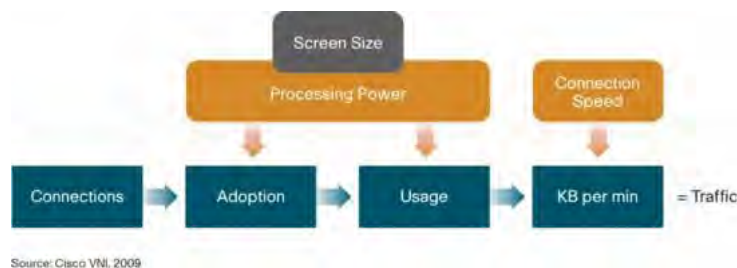
P2P traffic: 38% (worldwide)

Streaming video traffic: 27.7% (worldwide); 30.7% (United States)

Cisco regularly publish data on internet traffic and bandwidth usage within an ongoing research initiative known as the **Visual Networking Index**. The majority of published work within this initiative is based on the interpretation of analyst predictions about the future of internet usage. For these studies, Cisco state:

The core methodology relies on analyst projections for Internet users, broadband connections, video subscribers, mobile connections, and Internet application adoption. Analyst forecasts come from SNL Kagan, Ovum, Informa Telecoms & Media, Infonetics, IDC, Frost & Sullivan, Gartner, ABI, AMI, Screendigest, Parks Associates, Yankee Group, Dell'Oro, and Synergy.

Cisco produces data on the overall use of the internet for the VNI by combining these analyst predictions with an analysis of what are termed 'fundamental enablers' of internet usage such as broadband speed, computing power, and screen size, with the company positing a 'supply-side' aspect to internet usage as well as an end-user demand aspect.



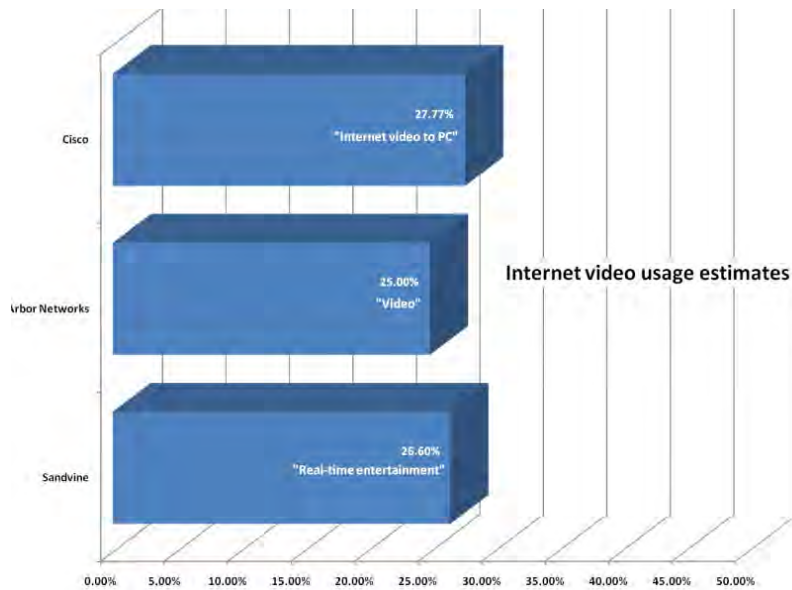
For the purposes of this study, Cisco's analysis is helpful as context but does not provide hard data based on the monitoring of actual internet traffic. However, Cisco also publish a Visual Networking Index **Usage Study** which draws data from over twenty ISPs worldwide serving a total of around 1m subscribers. This uses deep packet inspection to determine the type of data flowing into and out of each ISP.

Unfortunately, the amount of data publicly available from the Usage Study is low and in terms of categorising network traffic, only specific figures for file sharing usage are provided by the company.³⁸ This finds that **38% of global internet traffic can be identified as peer to peer**. The report also finds that "Nearly one-third of all file-

³⁸ The study also provides some data which states that the average broadband connection generates 11.4 gigabytes of Internet traffic per month and that the top 1% of broadband connections are responsible for more than 20% of total Internet traffic.

sharing Internet traffic is non-P2P. Web-based file-sharing, newsgroups, and FTP account for 32 percent of all file sharing traffic.” This means that in total, **55.9% of all internet traffic is what Cisco term file-sharing**. However, the data is not broken down by protocol or type of traffic – for instance, it is not known what proportion of the 38% that is peer to peer file sharing is produced by bittorrent or eDonkey; or how important ‘web-based’ file sharing is, nor exactly which sites are listed under that definition.

Cisco does provide significant detail within the main VNI studies, allowing data estimates to be broken down by country, type of traffic, and for a number of years going forward through a customisable web-based tool. However, as these estimates are based on analyst predictions (and as they differ from that produced within the actual Usage Study (for instance, peer to peer is listed as 31.7% in 2009 rather than 38%), their methodology makes them unsuitable for inclusion in this report. It is worth noting that the estimate for video streaming bandwidth use is very similar to that produced by Sandvine and Arbor, as the chart shows. Cisco defines this as “internet video to PC” and estimate it at 27.7% of all internet usage. This is relatively close to the estimates from Sandvine for ‘Real-time entertainment’ (26.6%) and Arbor’s ‘Video’ category (25.00%) – though again, note that the figures from Sandvine and Arbor are based on actual monitoring data rather than analyst estimates.



3.5 iPoque: Internet Study 2008/2009

Monitoring period: “Two weeks”, varied periods depending on location.

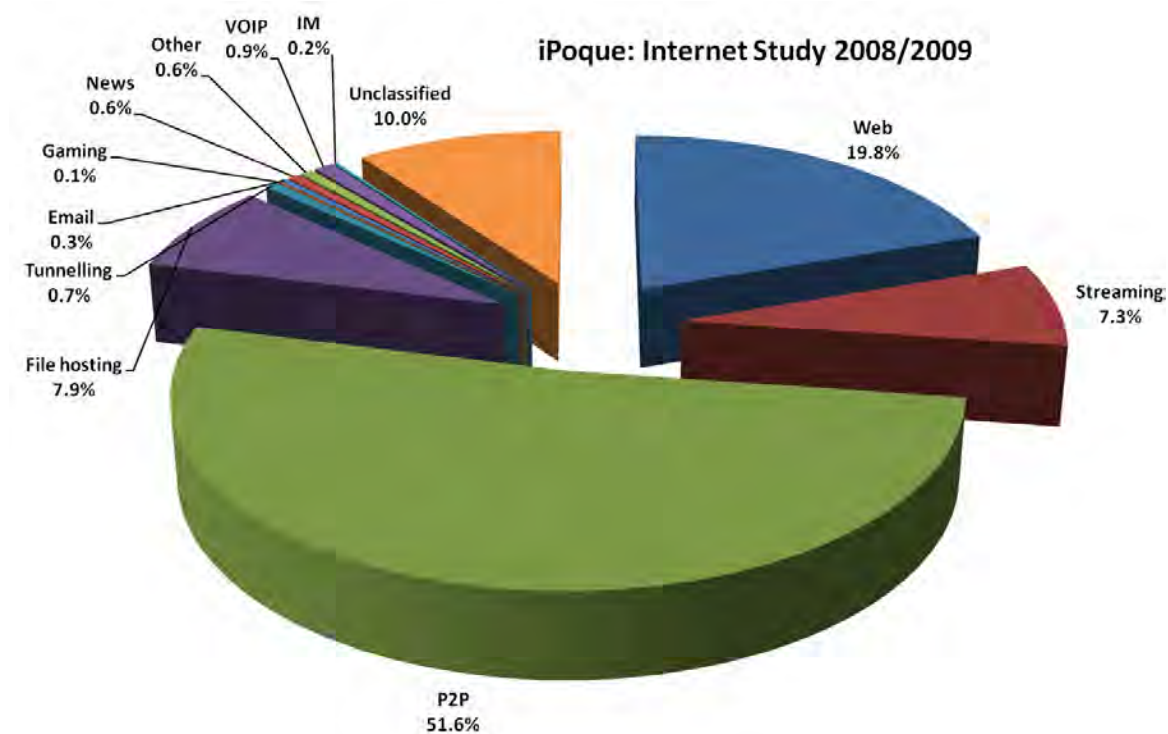
Monitoring locations: 11 monitoring locations; eight ISPs and three universities from eight regions: Africa, South America, Middle East, Eastern, Southern, and Southwestern Europe, Germany. No locations in the United States.

Number of subscribers: 1.1m

Amount of traffic monitored: 1.3 Petabytes (the smallest of the three studies where traffic amounts are known).

P2P traffic: 51.6%

Streaming video traffic: 7.34% (categorised as ‘Streaming’)



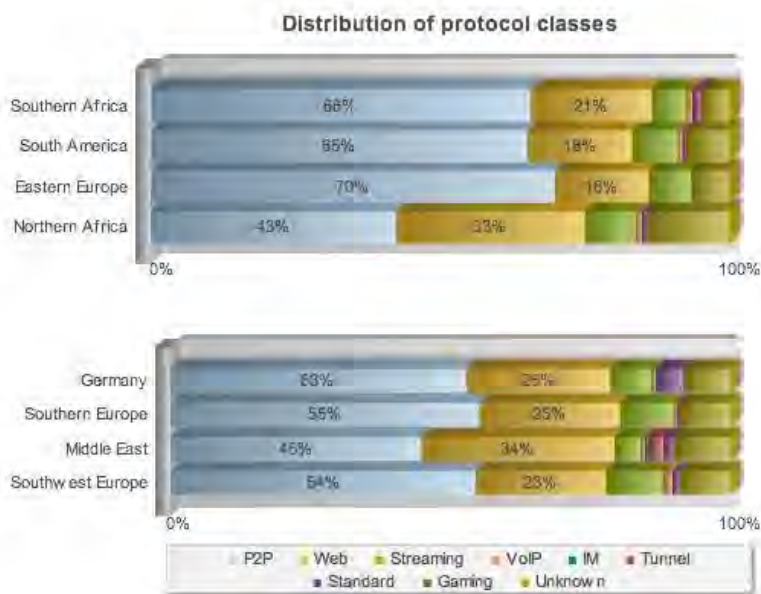
Other points:

- Peer to peer file sharing generates “by far the most traffic in all monitored regions” – from 43% in Northern Africa to 70% in Eastern Europe.
- Peer to peer traffic has dropped slightly as a proportion since their previous 2007 study. BitTorrent is the most popular single protocol.
- File hosting (direct downloads from cyberlockers) has increased to “up to 45% of all Web traffic” in some regions.
- “Rapidshare alone is responsible for 5 percent of the worldwide Internet traffic”.

3.5.1 Methodology

iPoque is a German network monitoring and DPI solutions provider. They claim to be the leading European company in their field. The company has issued 'Internet Study' reports each year since 2007. The 2009 report is detailed in its results and discussion but based on a small amount of traffic³⁹ generated from eleven locations at different (unknown) time periods and which cover a relatively small number of users (1.1m subscribers in total compared to 24m for Sandvine). Each location uses iPoque's PRX Traffic Manager hardware which combines protocol detection with DPI and behavioural traffic analysis.

The eleven locations themselves are scattered around Africa, Europe, and the Middle East, with only one or two locations in each country. Three of the locations are universities where user profiles and bandwidth usage are likely to be significantly different to a consumer ISP. The study notes that the various issues with the data (amount gathered, locations, types of network, time period, number of subscribers) mean that "the results are not statistically representative".



3.5.2 Discussion

The chart above, taken from the iPoque report, again shows the significant variation from location to location of different types of internet usage but also shows substantially different results – particularly for P2P usage – compared to the other three main studies.

³⁹ Arbor's study is based on over 200,000 times as much data.

- P2P is the highest single category in every region, ranging from 45% in the Middle East to 70% in Eastern Europe, far higher than other studies.
- Web use differs from 16% in Eastern Europe to 33% in Northern Africa.
- The 'streaming' category (defined by iPoque simply as audio and video streaming) takes up anything from 5.8% to 10.1% depending on location but does not come close to the one-quarter of internet traffic identified by the preceding three studies.

It is possible that the locations studied by iPoque simply represent areas which show significantly different internet usage to those monitored by Sandvine, Arbor, or Cisco. Previous reports from iPoque have historically shown much higher P2P usage than other monitoring companies: given the commercial focus of the company on the detection of file sharing protocols (and their equipment does appear able to detect an enormous range of protocols), it is also possible that iPoque may be able to detect some traffic which other monitoring companies might miss or be able to more accurately identify protocols. However, the variation is such that this cannot be the sole reason for the differences.

In summary, the iPoque report indicates that peer to peer traffic is very high in most of the monitoring locations from which they have obtained data while streaming is lower than shown in the other three studies. However, it is difficult to generalise from their findings to other locations and, in particular, to other countries. iPoque has good knowledge and capabilities in identifying different protocols but as a study of use in determining bandwidth make-up worldwide and in the United States, the report must be used with caution.

3.6 Focused studies

Two recent academic studies of network usage were also uncovered. Each examine only a single ISP and as such, the ability to generalise from the results will be difficult but each provide some findings worthy of discussion.

3.6.1 Maier et al (2009) - On Dominant Characteristics of Residential Broadband Internet Traffic

Maier et al. studied traffic for 20,000 subscribers from a major European ISP within a single urban area at various points during the second half of 2008 and the first half of 2009.

The study found that HTTP comprised 57.6% of all traffic with bittorrent responsible for 8.5% and eDonkey for 5% of traffic. At least one-quarter of all HTTP traffic carried Flash video with a further 7.6% carrying other video.

Just fifteen domains accounted for 43% of all HTTP traffic (and therefore 26% of all internet traffic). A single cyberlocker / direct download provider was responsible for 15.3% of *all* HTTP traffic (related to this, 14.7% of all internet traffic was in the form of RAR archives, commonly used in cyberlocker or newsgroup downloads).

Rank	Domain	Fraction of Traffic
1	Direct Download Provider	15.3%
2	Video portal	6.1%
3	Video portal	3.3%
4	Video portal	3.2%
5	Software updates	3.0%
6	CDN	2.1%
7	Search engine	1.8%
8	Software company	1.7%
9	Web portal	1.3%
10	Video Portal	1.2%

3.6.2 Erman et al. (2009) - Network-aware Forward Caching

Erman et al. examined internet traffic from 100,000 broadband subscribers from three states from a single broadband provider in the United States. The data analysed was taken at regular points from February 2007 to September 2008. The authors concluded that "HTTP... is increasingly being used to handle most of the Internet's tasks such as distribution of software, updates, patches, and multimedia, and by P2P applications".

- 66% of internet traffic was HTTP; the web is "the workhorse for data delivery"
- Video was a large portion of HTTP and around 22% of all traffic
- 12.3% was P2P (though this portion could be up to 17% given issues with identification)

3.6.3 Layton and Waters, *Internet Commerce Security Laboratory (April 2010) - Investigation into the extent of infringing content on BitTorrent networks*

This study was on the surface similar to the investigation pursued in Part A of this report into infringing content on bittorrent. The authors gathered data from a range of bittorrent trackers and collated the information, then looked at the most popular 1,000 individual files.

The authors found that 43% of the sample of 1,000 bittorrent swarms was films, 29% was television episodes, and 16.5% was music.⁴⁰ The proportion of torrents infringing copyright was estimated at 89% with no evidence of legitimate usage found in the torrents within the top three categories (film, television, and music).



However, the study had significant methodological flaws and as such, Envisional believes it should not be considered as valid for the purposes of this report.

- The authors chose the most popular 1,000 torrents in terms of **number of seeds** rather than number of downloaders. It is common for fake files or malware to have seed numbers artificially boosted in order to attract downloaders. Little or no work appears to have been done in weeding out the fake files, resulting in a peer count of over 117m seeds across only 1m torrents (compared to just 17m peers in *total* for all 1.8m torrents tracked by PublicBT in Part A).
- There was an issue with **domain pseudonyms** for common trackers. Some of the tracker names used in the data gathering actually point to an IP address for a different (and more popular) tracker altogether⁴¹.
- There are a number of instances where the **reported data** stretches credulity: for instance, at the point of their analysis in April 2010 the most popular file was listed as a pirated version of the film *The Incredible Hulk*. This film was released in 2008 and was not one of the most popular that year, yet the data produced by the authors state that one version for the film had over one million peers, both a level of popularity that is difficult to believe for a film of this age and an absolute number of downloaders that is higher than any single bittorrent swarm ever recorded by Envisional. For example, the number of seeds in the most popular swarm for the final episode of the television program *Lost* – believed to be the highest-seeded bittorrent swarm ever seen – was never above 100,000 at any one time, according to Envisional's own monitoring.

⁴⁰ http://www.icsl.com.au/files/bt_report_final.pdf

⁴¹ For instance, the tracker address "tracker.ilibr.org" points to the PublicBT tracker: a query to the ilibr.org tracker is actually sent to the PublicBT tracker instead. With both the ilibr tracker and the PublicBT tracker included in the data gathering, the same information is being gathered twice. Further, two versions of the ilibr.org tracker are included on two different ports - yet these both point to PublicBT and will end up querying the same tracker twice (the port numbers make no difference in this aspect).

3.7 Summary: Bandwidth Usage

As the preceding discussion makes clear, navigating through studies of internet traffic in order to attempt some level of consensus is challenging. With no established or accepted methodology, classifications, or measurement techniques, the analyst depends on the detail provided in each study to assign confidence and gain understanding.

Each of the four main studies discussed have methodological issues of a greater or lesser extent.

- **Sandvine's** report is detailed but the amount of traffic on which the analysis is based is not provided. Given that the focus is upon three weeks of analysis across 24m ISP subscribers, the data volume should be significant. Further, the methodology is outlined clearly and the company was also willing to discuss their approach and send further data when requested.
- The **Arbor** study is based on a volume of data which dwarfs all other studies but detection is poor and while a smaller dataset is analysed to allow more precise measurement of certain sectors, confidence is obviously affected.
- **Cisco** provides only a few data points. Their main VNI reports provide granular data for a wide range of applications and countries yet rely on analyst predictions rather than data measurement. The focus is much more on predicting network growth than on detailing traffic for a particular time period.
- **iPoque's** report relies on a limited sample of data from varied dates across a small range of monitoring locations in less developed internet markets.

Apart from Arbor who do not analyse traffic in this manner, all studies show significant regional variation. Internet usage in North America is clearly not the same as in Latin America or Europe or Asia. The variations shown for instance by iPoque across monitoring locations in the same small region demonstrate that there can be large variations between countries (and likely within countries, also). Envisional's own monitoring data for networks like bittorrent and eDonkey show differences between countries in usage of those protocols.

With the limitations of each study in mind, it does seem possible to generate some broad conclusions and estimates about internet traffic using the data provided.

3.7.1 The importance of the web

- Standard, daily, routine **web browsing** – to Google, Facebook, the BBC, Wikipedia, Twitter, Amazon, eBay, Flickr, blogs, forums, and so on – is responsible for around **one-third of all internet traffic**. It may be difficult to be more precise than this: so many applications and sites employ the web for distribution or storage of content that categorisation becomes difficult. Sandvine and Cisco appear to ensure that most web traffic which is not web-page based (such as video streams, file hosting downloads, and so on) are



Web: 33%

categorised separately but the two studies diverge significantly over how much traffic is then left: Sandvine posits 33.7%; Cisco's VNI study estimates just 18.2% (a figure which also includes email and instant messaging data). Arbor finds that 42% of internet traffic is 'Web' while iPoque estimates anywhere from 16% to 34% depending on location (with

this figure including file hosting sites). The smaller Maier and Ermann studies find around 35% of traffic to be non-video HTTP traffic. For this report, the amount of web usage is held to be 33% of all internet traffic.

- In the **United States**, the maturity of the web and its place as home to so many applications which have extended the use of the web – Google, YouTube, Facebook, Twitter, and so on – mean that relative web use in the US may be higher than that observed worldwide. Both Sandvine and Cisco (the only two of the four studies to analyse the US or North America separately) report or estimate slightly higher web use in the country.
- Beyond everyday web browsing, there are two other areas of web-based traffic which should be considered separately: **streamed video** (and to a lesser extent, audio); and **file hosting** or cyberlockers.
 - **Video content**, particularly streamed video, is one of the major components of internet traffic, with much of it being transmitted through or sourced from HTTP communication. Three of the studies reach a broad level of consensus on the level of internet traffic which features streamed content: Sandvine's 'Real-time entertainment' category, Cisco's 'Internet video to PC' estimate, and Arbor's simple 'Video' category all place web-based video viewing at around **25%-28% of traffic** (and is assumed to be 26.5% for the purposes of further analysis in this report). Sandvine's category includes audio-only streams and Arbor's category is hardly defined at all but the figures are relatively close in agreement. This is an area where the iPoque study shows considerable difference to the other three reports. It is possible that streamed video is less important in the locations where their measurement technology is based but without further detail on the countries from which iPoque are reporting, this can only be speculation.

Video: 25-28%

On-demand video content appears to be consumed more highly in the **United States** (the home of YouTube and many other online video hosts) than in other regions: ComScore reported that over 173m internet users in the US watched more than 32bn videos during January 2010 alone, significantly higher figures than for users in Germany and France, for instance. With this in mind, an estimate for video usage in the United States as comprising 27%-30% of internet traffic can be made.

- The use of central web-based **file hosting sites or cyberlockers** such as Rapidshare and MegaUpload can be significant depending on country. These sites seem to be more heavily used in Europe and less developed internet markets (such as the Middle East and Africa) than they are in North America. Sandvine estimate that cyberlockers are responsible for around 5.3% of all internet traffic, and this should be seen as a minimum – the company's list of sites included in the 'Storage and backup' category is far from exhaustive for cyberlockers. However, no other cyberlockers are as large as Rapidshare and Sandvine provides detailed traffic analysis for that site and for MegaUpload. Thus while actual cyberlocker usage may be higher than Sandvine's figure, it is likely not much higher. iPoque believe that Rapidshare alone contributes 5% of all traffic and that cyberlockers overall are responsible for 7.9% of traffic though this comes from countries where cyberlocker usage appears to be relatively high. Cisco do not delineate this area specifically but do estimate 'non-P2P' filesharing (web-based file sharing, newsgroups, and FTP) at around 19%. It is reasonable to assume that most of this non-P2P filesharing will be from cyberlockers as newsgroups and FTP are shown in other studies to be around

*File hosts /
cyberlockers: 7%*

1% of all internet traffic and little more. As with their estimate for peer to peer usage (see below), Cisco are therefore estimating a much higher level of cyberlocker usage.

Arbor are fairly quiet on this issue, stating only that MegaUpload was found to be responsible for around 0.6% of all internet traffic in early 2009.

Analysis of the overall data available leads to a cautious estimate that central file hosts like cyberlockers are responsible for around **7% of internet traffic**.

Data from Sandvine – the only source of information on this area – show relatively low usage of the two main cyberlockers for users from North America. Given this, an estimate of cyberlocker usage for the United States of **3%** is acceptable.

3.7.2 Peer to peer remains significant

- **Peer to peer applications** have traditionally been considered to take up a very large amount of internet traffic: studies from 2005 found that more than half of all internet traffic used peer to peer. That may have been correct at that time but as noted above, there has since been a resurgence of the importance of the web to internet users at the same time as the internet has become increasingly a video-based medium. This is not to say that peer to peer traffic is declining in absolute terms.

Determining how much internet traffic is peer to peer is more difficult. The proportion varies from study to study and, within those studies, from region to region, but it is likely that at least 20% of all internet traffic comes from peer to peer applications. Sandvine's figure is 20.4% worldwide and this may be slightly low. The list of P2P protocols included in their study is not exhaustive, though does include the major networks. However, both iPoque and Cisco place P2P usage much higher: the former at over 51% and the latter at 38%. iPoque's figure can only be taken as evidence of P2P usage in the particular locations they monitor. Cisco's figure is from a relatively small sample of 1m subscribers but accords with the higher figure they estimate from analyst predictions.

*Peer to peer:
25%*

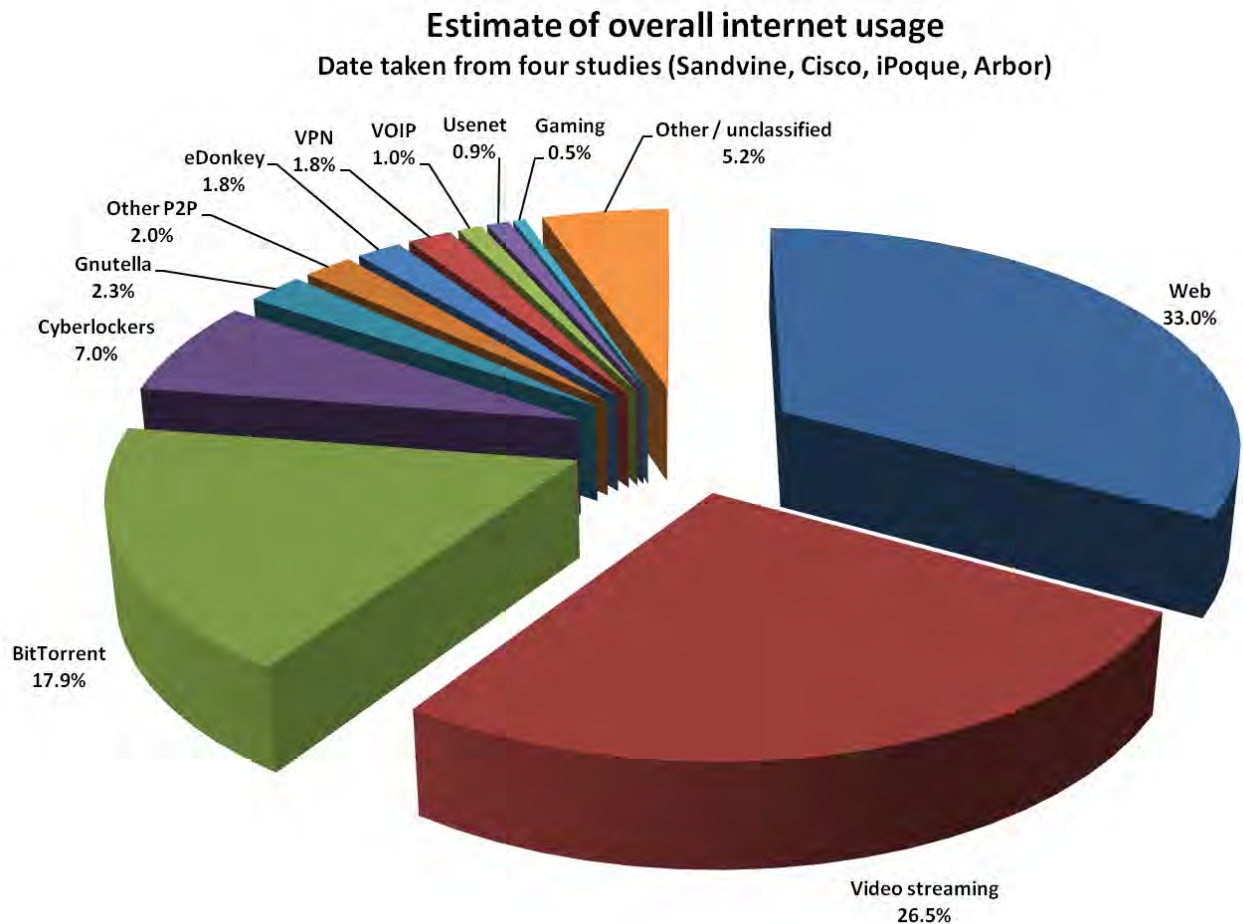
Given these issues, this analysis estimates P2P usage worldwide at **25%** of all internet traffic. On this reading, bittorrent uses around 17.9% of all internet bandwidth.⁴²

- The **United States** appears to be one of the lowest relative users of peer to peer worldwide: Sandvine measure aggregate (downstream and upstream) peer to peer traffic at 18.5% in North America and 14.6% for downstream, mostly through bittorrent. Similarly, Cisco's estimate falls from 31.7% for worldwide P2P usage to 23.9% for the United States alone. There is thus less of a gap between the two studies to reconcile. Assuming US P2P usage to be around **20% of internet traffic** seems reasonable with bittorrent at 14.32% and other peer to peer traffic accounting for just over 5%.

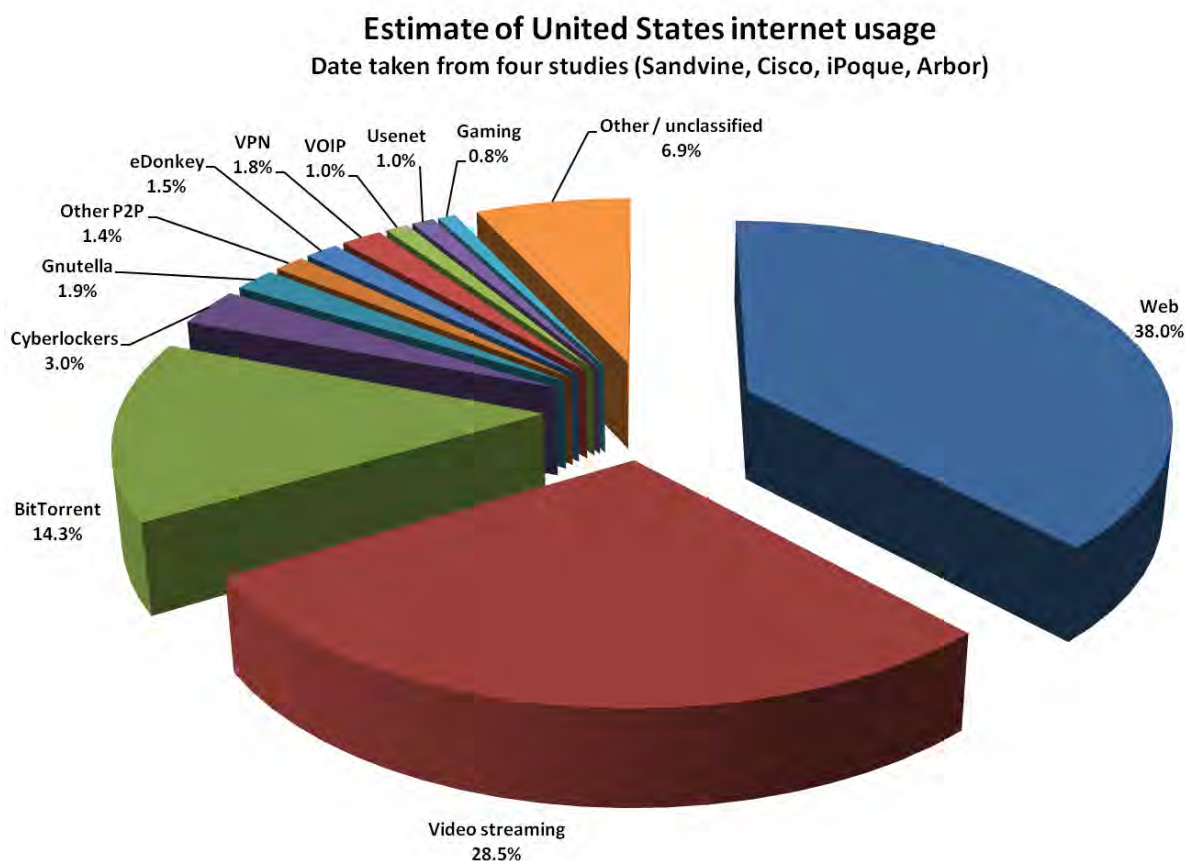
⁴² Only Sandvine provide an overall figure for the amount of network traffic for which bittorrent is responsible: 14.1% (or 71.6% of all peer to peer traffic). If Sandvine's peer to peer estimate of 20.4% is taken as slightly low and the figure of 25% is assumed for all peer to peer data, then the overall figure for bittorrent would be extrapolated to 17.89% of all internet traffic.

3.7.3 Overall estimate

The chart below uses Envisional's own analysis experience and internet intelligence to draw together the four monitoring studies in order to produce an overall estimate for internet bandwidth usage. Web traffic and video streaming (most of which takes place through the web or via HTTP) makes up almost 60% of all bandwidth. BitTorrent provides another 17.9% with peer to peer overall contributing 25% of internet bandwidth. Areas of internet usage such as VPN tunneling, voice over IP, and gaming, are estimated by each of the four monitoring companies to contribute much smaller amounts of overall bandwidth.



In the United States, the higher relative use of the web and video streaming means that these two components are responsible for two-thirds (66.5%) of all bandwidth. BitTorrent usage is slightly lower at 14.3% with other peer to peer protocols contributing a further 5.7% of internet bandwidth. Cyberlocker usage is estimated to be lower in the US than elsewhere in the world, while Gaming and Usenet consumption is very slightly higher.



Part C of this report brings together these overall estimates from Part B with the analysis of common piracy arenas found in Part A to provide an estimate of the amount of internet traffic overall which is believed to be infringing.

4 Part C: Drawing the data together

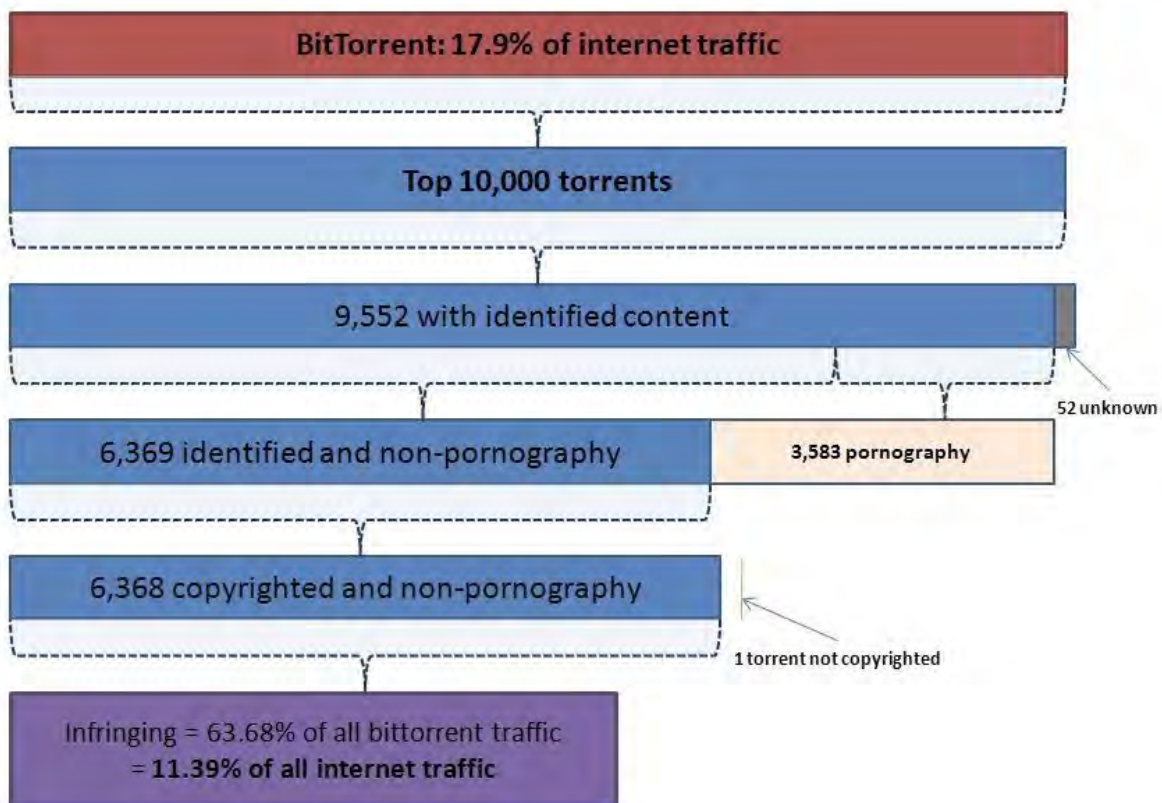
4.1 Introduction

Part A of this report examined a range of common internet arenas where pirated activity is often found and attempted estimates of the level of infringing activity found within each. Part B critically assessed four studies that attempted to determine the amount of overall internet bandwidth used by different protocols and types of content.

This final part of the report brings together these two parts in an attempt to provide an overall estimate for the amount of all internet traffic likely to be infringing. Each of the common piracy arenas examined in Part A will be summarised in turn.

4.2 Estimates of infringing use

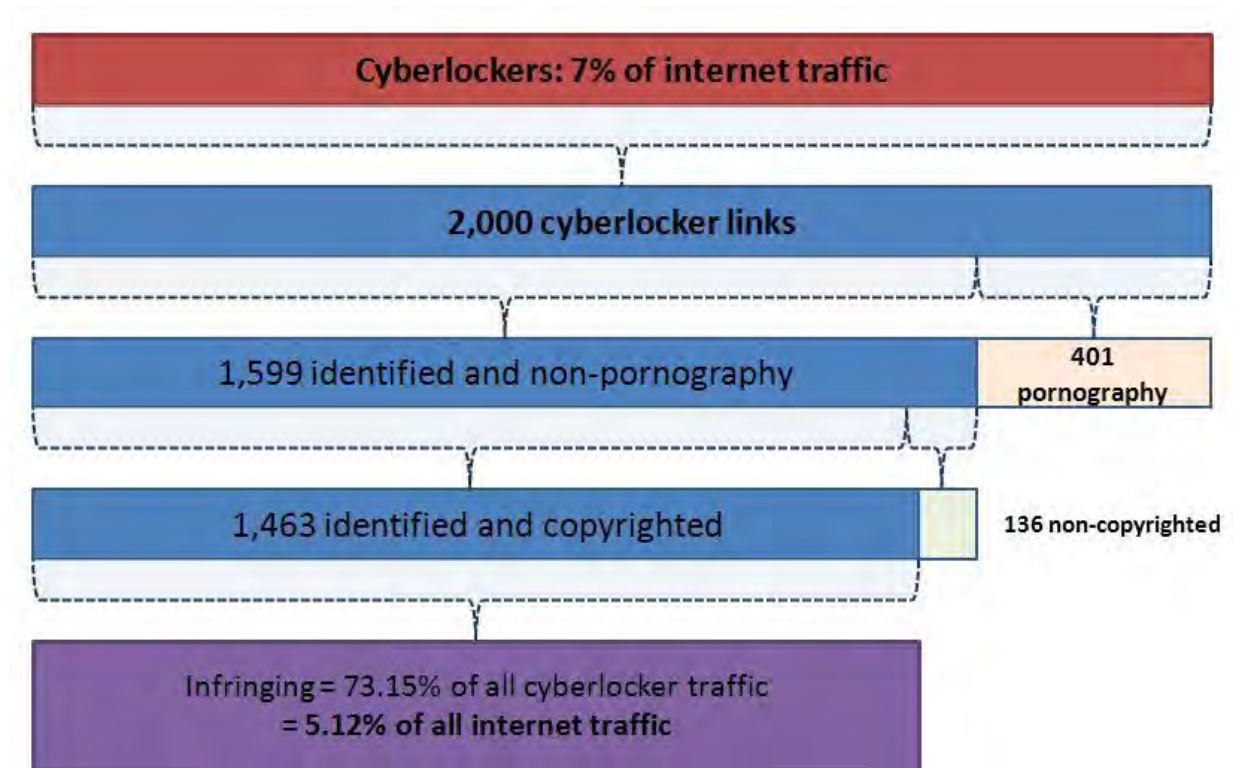
4.2.1 BitTorrent



The chart for bittorrent starts with the estimated 17.9% of internet bandwidth which is believed to be bittorrent. The amount of that bandwidth deemed to be infringing is estimated by reference to the analysis of the most popular 10,000 torrents held on PublicBT (found in Part A of this report). 63.68% of these torrents were found to be infringing and not pornography. This means that 63.68% of the internet bandwidth consumed by bittorrent can be estimated to be of infringing content, resulting in a final estimate that **infringing use of bittorrent is responsible for 11.39% of all traffic on the internet.**

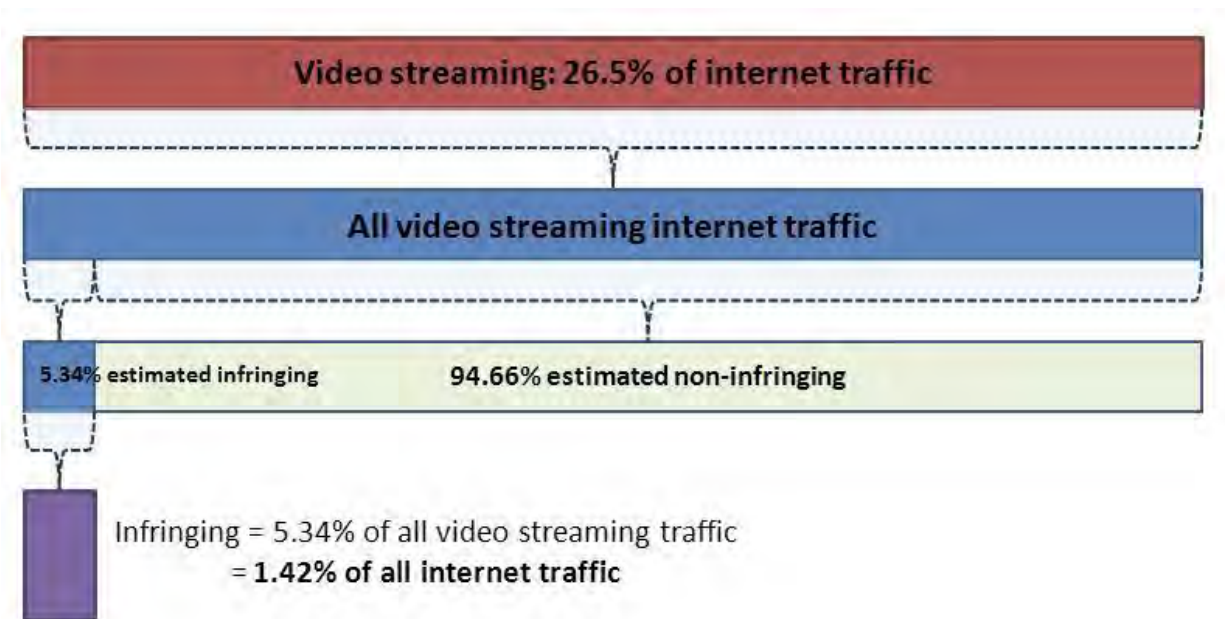
4.2.2 Cyberlockers

Cyberlockers are estimated to be responsible for 7% of all internet traffic. The estimations produced in Part A lead to a belief that around 73.15% of traffic to cyberlockers is related to infringing content. With an estimated overall internet bandwidth usage of 7% down to cyberlockers, this leads to an overall estimate for **infringing use of cyberlockers as 5.12% of all internet bandwidth.**



4.2.3 Video streaming

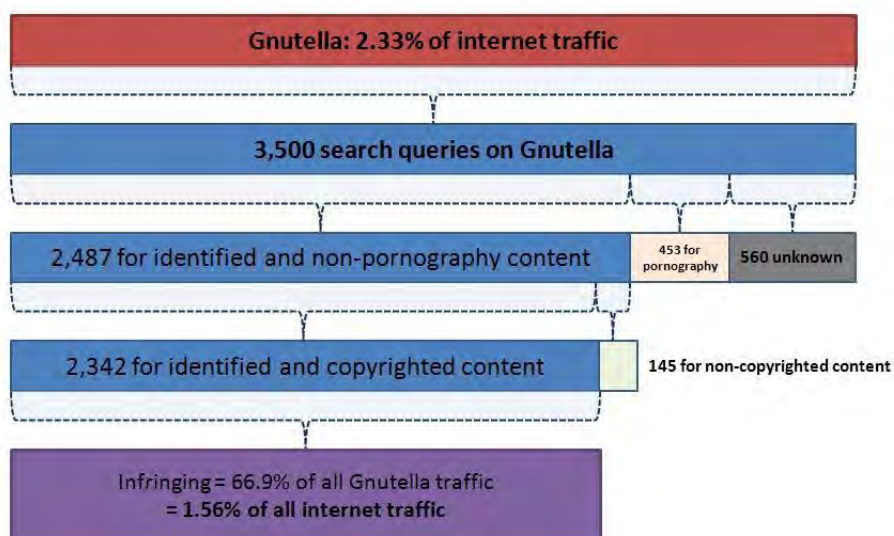
As Part A showed, the largest proportion of video streaming usage is legitimate and non-infringing. The studies discussed in Part B also demonstrated that video streaming traffic is the fastest growing area of internet consumption and is already responsible for more than one-quarter of all internet usage. As such, despite only 5.34% of all video streaming traffic estimate as infringing, this still amounts to **1.42% of all internet traffic**.



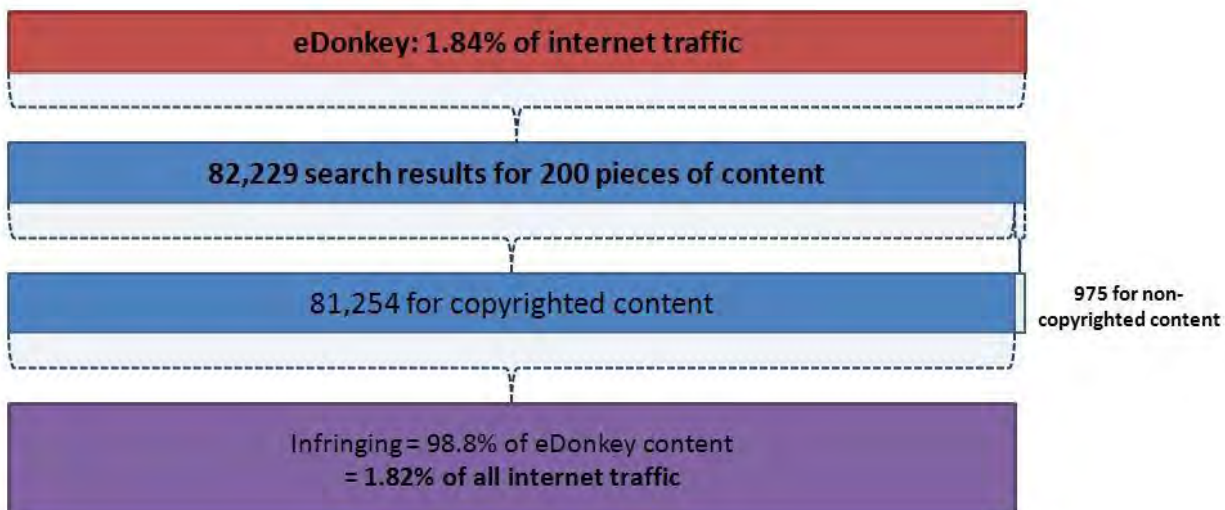
4.2.4 Other piracy arenas

Three other common piracy arenas were analysed in Part A: Gnutella, eDonkey, and Usenet.

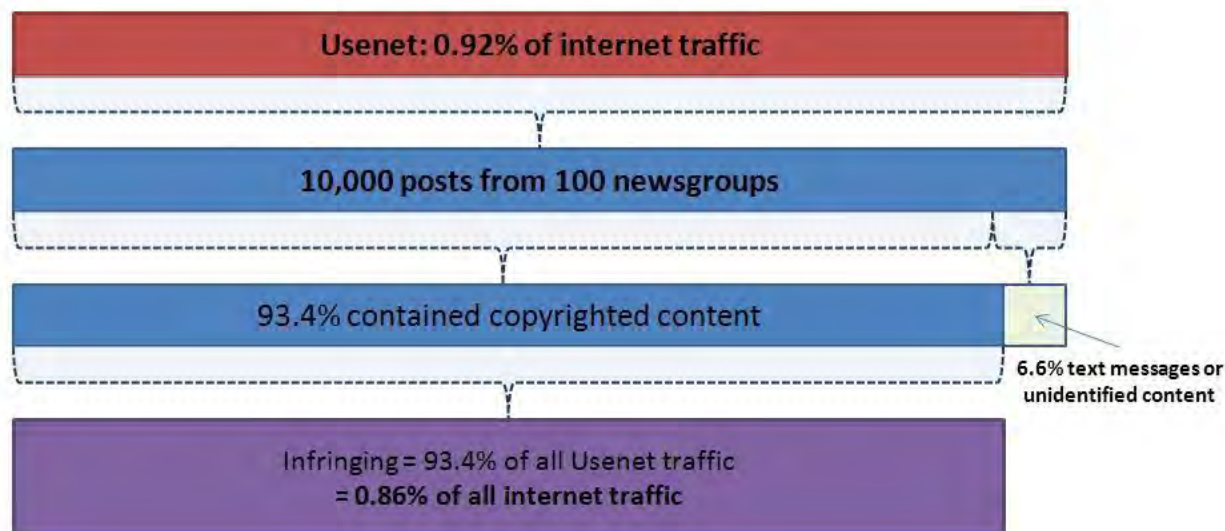
Gnutella is believed to be responsible for around 2.33% of internet traffic worldwide. With 66.9% of content searched for on the network estimated to be infringing and non-pornography, this leads to an estimate of **1.56% of internet traffic contributed by infringing content on Gnutella**.



eDonkey is heavily used in continental Europe, though it has declined in usage over the last two to three years after a series of successful anti piracy actions. The estimate in Part A is that 98.8% of eDonkey content is infringing. With 1.84% of internet traffic believed to be eDonkey, this would mean that **1.82% of all internet traffic is infringing content on eDonkey.**



Part A estimated the proportion of **Usenet** content that was infringing at 93.4%. The best estimate possible from the four studies in Part B found that Usenet made up 0.92% of all internet traffic. This would produce an overall estimate for the amount of infringing internet traffic from Usenet of 0.86%.



Other P2P or file sharing networks also exist which are not explicitly covered within this research, such as Ares, DirectConnect, Kad (a sister network to eDonkey), Gnutella2 (used by clients like Shareaza), and MP2P (used by Piolet and Blubster), for instance. The four monitoring studies lead to an overall estimate for peer to peer usage other than the networks already discussed above of **2.02%**.⁴³ It will be assumed that infringing use of these networks is similar to the average infringing use of the networks analysed here in more detail: 78.94%. This would lead to an estimate of **overall internet use contributed by infringing content on these networks of 1.6%**.

Other types of internet traffic may also be used for infringing purposes. For instance, unauthorised copyrighted content might flow across VPN traffic and some VPN services like Relakks in Sweden exist primarily to hide file sharers from detection. Infringing content might also be transferred across email or be downloaded from normal web sites or blogs, for instance – though this would usually be small pieces of content such as music files rather than anything larger. However, estimating the size of this infringing traffic is extremely difficult, though experience means that the amount is likely to be small relative to the overall amount of bandwidth estimated for each type of traffic. As such, infringing content in these other areas is discounted for the purposes of this report, though this should not be taken as an indication that they are not used for the purposes of infringement.

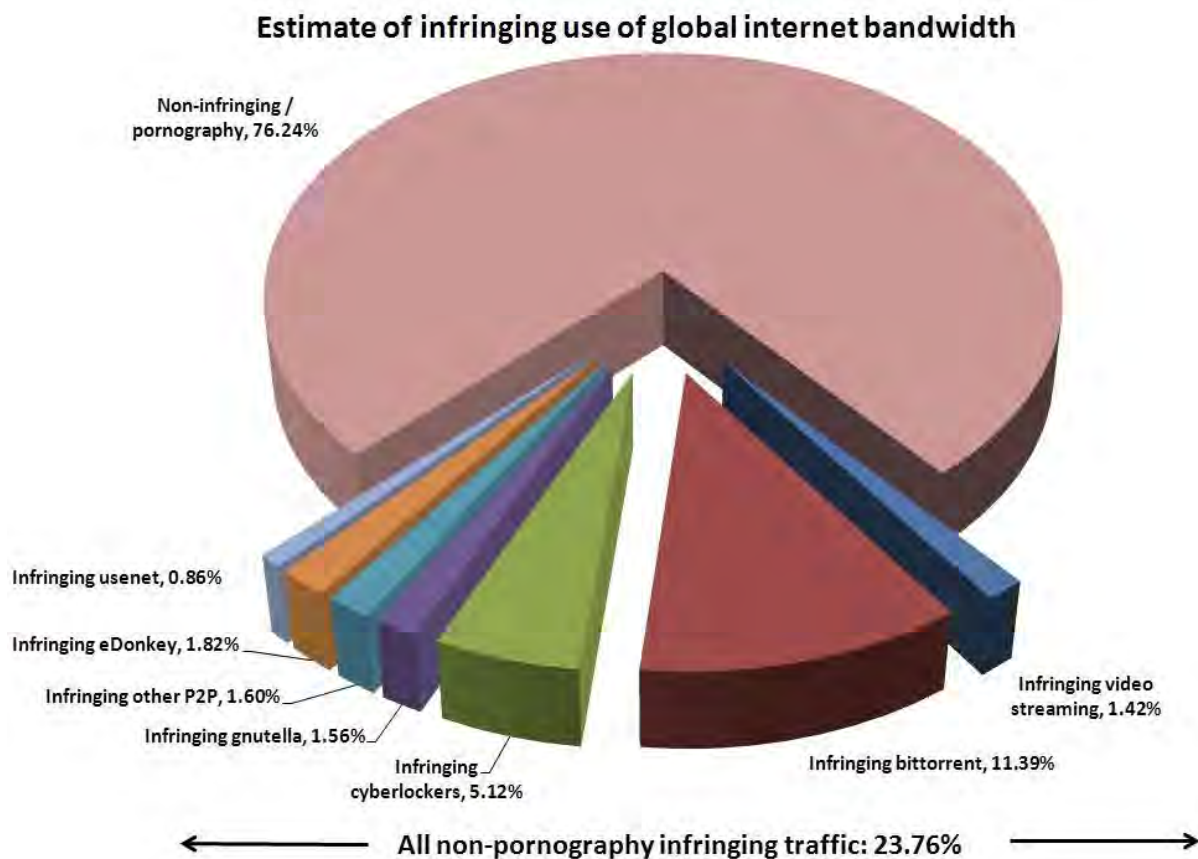
⁴³ A figure derived by taking the overall estimate for peer to peer traffic and subtracting the networks already identified (bittorrent, eDonkey, and Gnutella, for instance).

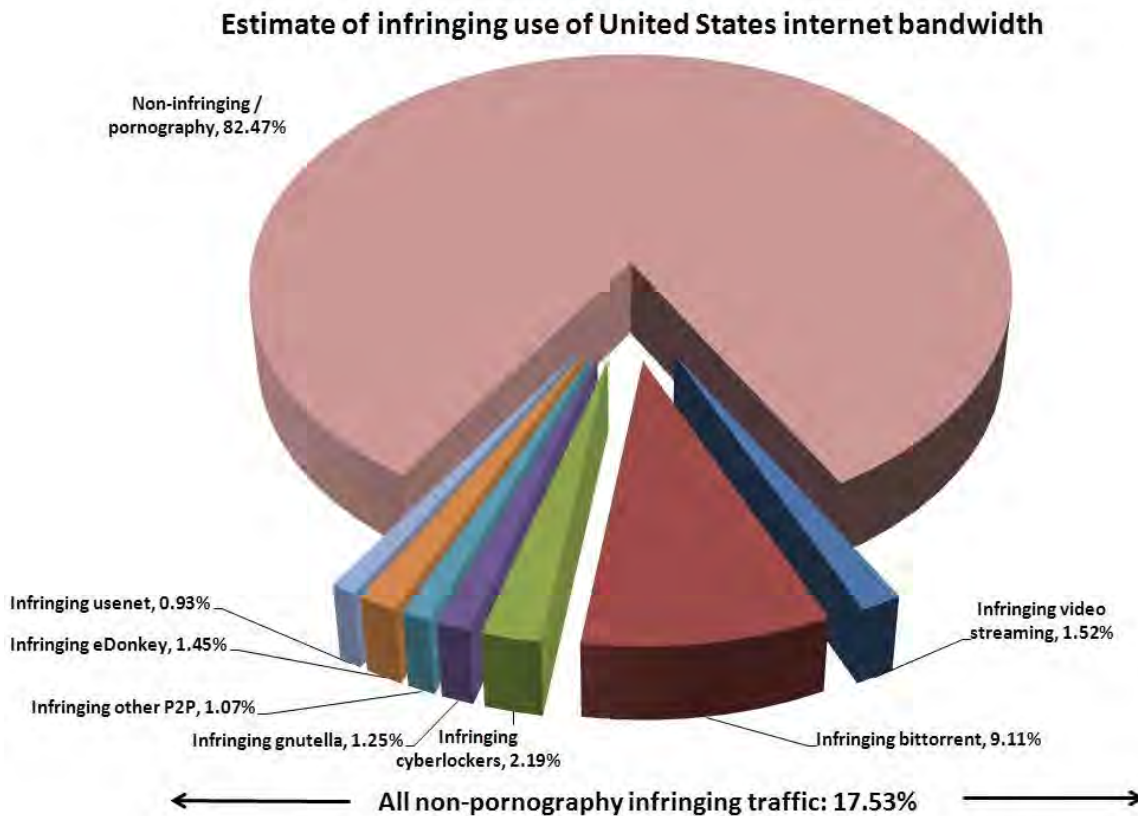
4.3 Summary

This report attempts to produce an estimate for the proportion of traffic which crosses internet that infringes copyright. Using studies of overall internet usage and analysis of common arenas through which content is transferred on the internet, the report finds that it is possible to calculate that a minimum of **23.76% of all internet bandwidth is devoted to the transfer of infringing and non-pornographic content.**

In the United States, the transfer of infringing and non-pornographic content is estimated to be responsible for a minimum of **17.53% of all internet bandwidth.**

The charts below show the overall estimate for the amount of global internet bandwidth which is believed to be infringing (and not pornography) and the overall estimate for the amount of United States internet bandwidth.





These estimates must, obviously, be issued with numerous caveats, both about the quality and accuracy of the data offered by the monitoring companies which estimate overall internet usage and about the ability to precisely quantify the proportion of infringing content on each arena of the internet. Methodological issues abound in both areas. Yet even given the limitations of the data available, Envisional believes that the estimates produced in this report are more accurate than any that have been published before. This report draws together the data in a way that allows, for the first time, the organisations which can help shape the ways in which users interact and obtain content to understand how much of the internet is devoted to the distribution and consumption of infringing material.

Piracy Intelligence

Envisional Ltd

